

SOCIO-LEGAL PERSPECTIVES ON CYBERSPACE



Xingan Li

LLB, LLM, LLD, PhD, School of Governance, Law and
Society, Tallinn University, Estonia



Toronto Academe Press

SOCIO-LEGAL PERSPECTIVES ON CYBERSPACE

Xingan Li

LLB, LLM, LLD, PhD

School of Governance, Law and Society

Tallinn University, Estonia

TORONTO ACADEME PRESS

©2016 Xingan Li. All rights reserved. No part of this book shall be reproduced, stored in a retrieval system, or transmitted by any means – electronic, mechanical, photocopying, recording, or otherwise – without written permission from the publisher.

Made in Canada

Title: Socio-Legal Perspectives on Cyberspace
First Edition, June 2016

ISBN 9780973981308 (PDF)

Publisher:
Toronto Academe Press
670 University Ave.
Charlottetown PE
C1E 1E3



Toronto Academe Press

ACKNOWLEDGEMENTS

The editor and publishers wish to thank the following for permission to use copyright material.

Li, Xingan (2015). Cyberspace and the Informed Rationality of Law. *The Romanian Journal of Sociology*, 26, 3–27. ©2015, Xingan Li.

Li, Xingan (2014). Exploring into regulatory mode for social order in cyberspace. *Webology*, 11 (2), 1–8. ©2014, Xingan Li.

Li, Xingan (2010). Legal-Service-Oriented Architecture (LSOA) in E-lawyer. *Lex et scientia*, 17 (1), 196–203. ©2010, Xingan Li.

Li, Xingan (2014). Phenomenal exploration into impact of anonymity on law and order in cyberspace. *Criminology & Social Integration Journal*, 22 (2), 102–123. ©2014, Xingan Li.

Li, Xingan (2006). Cybersecurity as a Relative Concept. *Information & Security: An International Journal*, 18, 11–24. ©2006, Xingan Li.

Li, Xingan (2008). The Criminal Phenomenon on the Internet: Hallmarks of Criminals and Victims Revisited Through Typical Cases Prosecuted. *University of Ottawa Law & Technology Journal*, 5, 125–140. ©2008, Xingan Li.

Li, Xingan (2006). E-marketing, Unsolicited Commercial E-mail, and Legal Solutions. *Webology*, 3 (1), 1–15. ©2006, Xingan Li.

Li, Xingan (2007). The Phenomenon of Unsolicited E-mails with Attachments. *SIMILE: Studies In Media & Information Literacy Education*, 7 (2), 1–11. ©2007, Xingan Li.

Li, Xingan (2009). Extension of Victimization in Unsolicited E-mail Messages with Attachments (UEMAs): An Explanation of Seeking and Exposing Process. In Xingan Li, *Social Order in Cyberspace*. Hyderabad, India: ICFAI University Press, -©2009, Xingan Li.

Li, Xingan (2005). Spam Solutions: A Law and Economics View. *Asian and Comparative Law*, 3 (1), 54–64. ©2005, Xingan Li.

Li, Xingan (2010). Cyber Warfare: Jokes, Hoaxes, or Hypes. *The IUP Journal of Cyber Law*, 9, 7–16. ©2010, Xingan Li.

Li, Xingan (2016). regulation of cyberspace: Chinese law on cybersecurity and cybercrime. International Journal of Cyber Criminology (forthcoming). ©2016, Xingan Li.

Li, Xingan (2007). International Actions against Cybercrime: Networking Legal Systems in the Networked Crime Scene. *Webology*, 4 (3), 1–15. ©2007, Xingan Li.

PREFACE

The purpose of this book is to present thirteen of my articles in a collection form. This is necessary because there are important ideas that are easily understood as integrity. Themes of these articles are focused on socio-legal issues of cyberspace. The following sketches a whole picture of the contents.

Chapter I is an article for tentative description of cyberspace and informed rationality of law. Pervasive use of information system forms an irresistible force in shaping nearly all lives of our society. It poses great challenge to the previous legal system and requires special attention from the academic field. The purpose of this article is to identify potential change of legal systems in cyberspace, and to deal with the correlation between enhancement of legal literacy and the informed rationality. The article applies Weber's two dimensional coordinate system comprised of "formality" and "rationality" and expands it into a three-dimensional model by distinguishing "informability" and "uninformability". The article also considers the relationship between internal and external control over the cyberspace order. Finally, the article discusses the infeasibility of the idea of computerized justice system.

Chapter II is an article exploring into regulatory mode for social order in cyberspace. An increasing necessity for building social order in cyberspace through legal instruments has existed as one of many alternatives to regulate the world dominated by the globally connected Internet. This article discusses legal gaps of cyber-laws among different localities, with special regards to regulation over Internet content, through an approach with emphasis on players in three different steps of data movement that are separately characterized by human-machine, machine-machine and machine-human interaction with different degrees of human intervention. From the features of each stage, it is

concluded that official action must be within the ability of the controller so that it can be effective, and that it must also cope with the utility of the controller so that it can be efficient, so that an ability-and-utility-oriented control mode would ideally functions.

Chapter III is an article on Legal-Service-Oriented Architecture (LSOA) in eLawyer. Legal services have long been practiced under a monopolistic mode, face-to-face consultation between lawyers and clients being the prototype. Pervasive use of information systems provides the possibility for clients to access legal services in a more cost-effective way. eLawyer is an electronic system assisting lawyers to provide and clients to receive legal services. In this paper, I would like to introduce current development in the respect of eLawyer. In this paper, a broad outlook on legal service is applied, and I will give some basic ideas about how the eLawyer should be structured and operated, which parties are involved, what kind of relationship they have, what services they transact, and what limitations there are in eLawyer services.

Chapter IV is an article on phenomena exploration into impact of anonymity on law and order in cyberspace. While information systems provide modern society with great convenience, it also poses new problems in maintaining social order. One of its negative influences is the anonymity of cyberspace, which makes identity tracing a noteworthy predicament which poses obstacles in detection and investigations. It has been found that cyber anonymity has critical impacts on criminal motivation, and the phenomena of victimization, and should be tackled on different layers including technology and law enforcement. The article explores how the anonymity symbolizes the cyberspace, what threats are posed by cyber anonymity against social order, what potentialities the anonymity has, how the transterritorial anonymity was facilitated, and the real impact of anonymity on law and order in the information society.

Chapter V is an article on cybersecurity as a relative concept. Based on the relativity of the concept of cybersecurity, this article analyzes the economic impact of cybersecurity breaches, identifies cybersecurity as a private good that should be provided mainly by the private sector. However, public provision is also necessary when severe security breaches occur and liability mechanisms should be triggered.

Chapter VI is an article on the criminal phenomenon on the Internet: hallmarks of criminals and victims revisited through typical cases prosecuted. With the growth of research on cybercrime, increased attention has been given to the hallmarks of cybercriminals and the security levels of cybervictims by lawyers and law enforcement officials. The purpose of this study is to present an

updated profile of cybercriminality and cybervictimization based on empirical methods. The study uses a sample of 115 typical cases prosecuted between 18 March 1998 and 12 May 2006, which were published on the official website of the United States Department of Justice. The study found that males are responsible for a majority of these cybercrimes. Cybercriminals are primarily between the ages of 17 and 45. Domestic perpetrators constitute the absolute majority of the cybercriminals. Outsiders are four times more likely to be involved in cybercrimes than insiders. Most cybercrimes did not involve monetary loss, while those that did caused an average of one million dollars in damage. The most vulnerable interests are in the private sector. The security measures taken by victims are surprisingly weak, and are vulnerable to uncomplicated cybercrimes. The punishments (both imprisonment and fines) for cybercrime are generally light.

Chapter VII is an article on e-marketing, unsolicited commercial e-mail, and legal solutions. The purpose of this paper is to explore the legal solutions to unsolicited commercial e-mail. The advantages of e-mail enable it to be one of the most important e-marketing instruments. Spammers are also motivated by potential profits in spamming. The low costs and high benefits of the spammers, and the high costs and low benefits of the spammed determine the illegal nature of the spamming. The spam poses challenges for e-mail recipients' property rights, fair trade, public morals, cybersecurity, personal data protection, and involves other concerns as well. In dealing with spam, technical and marketing solutions cannot work alone without the legal mechanisms. The legal regulation is justified by balancing the interest between senders, service providers and even users. Criminal sanctions, civil remedies, and international harmonization are alternative steps in establishing legal solutions. As a necessary part of the legislation, punishment for unsolicited commercial e-mails should be more severe. Still, there are a number of limitations to the effectiveness of law enforcement against spamming. Spam must be eliminated by comprehensive mechanisms.

Chapter VIII is an article on the phenomenon of unsolicited e-mails with attachments. Unsolicited e-mails became prevalent with the growing penetration of computer networks. The senders of unsolicited e-mails make every effort to get the attention of the recipient. The goal is for their messages and/or attachments to be opened. The victimization of recipients of unsolicited messages with attachments happens without the recipients actually accessing their e-mail accounts. The victimization-conspiracy model happens when the messages include contents offering products or services that need illegal involvement of the recipients. The recipients of messages with such offers are first victimized by the unsolicited messages; and if they accept the illegal services or purchase the illegal products, they are likely to become the co-conspirators of the senders. The senders and the

recipient would reach an illegal double win effect. The unsolicited messages with attachments provide e-mail users many different options. The majority of messages in this study, however, offered recipients two alternatives; to conspire in tax evasion, or to be damaged by viruses.

Chapter IX is a following study of the previous article, on extension of victimization in unsolicited e-mail messages with attachments (UEMAs): an explanation of seeking and exposing process. While the growing scale of Internet use brings about great convenient for users, phenomena of unsolicited e-mail pose new threats and challenges. Previous literature was concentrated on general analysis of such messages, leaving many particular respects untouched. This study focuses on the extension of victimization of unsolicited messages email with attachments (UEMAs). Based on the analysis of two samples, one comprised of 501 (sampling done in May 2006), and the other comprised of 490 (sampling done in March 2008), pieces of UEMAs, the study finds that e-mail account exposing and seeking can both contribute to victimization; while receiving of unsolicited messages is the initial victimization, reading and reacting to messages could lead to additional victimization from virus attack or financial fraud, and from conspiracy in illegitimate operations such as tax evasion or transaction of falsified documents.

Chapter X is an article on spam solutions: a law and economics view. The paper begins with a precise description of the phenomenon, and continues in section II to classify the Spam. In Section III, the paper lists the problems brought about by Spam, such as fraud and deception, pornography, security implications and identity theft. Section IV gives a sketch of the scale of Spam. Section V is an analysis of the costs and benefits of sender and recipient of Spam. The paper examines effect of the four primary solutions, including technological, market, educational and regulatory in Section VI and VII. Special reference is placed on the economic analysis of different regulatory modes. At last, the paper ends with conclusions that Spam must be eliminated by comprehensive mechanisms.

Chapter XI is an article on cyber warfare: jokes, hoaxes, or hypes? Cyber warfare is increasingly listed alongside nuclear, chemical, and biological weapons as a potential weapon of mass destruction. Interest in and concerns for cyber warfare have also been prevalent for decades. War-oriented writer usually exploited such serious and expensive terms as cyber war, information war, and electronic war to spread their impetuous and cheap ideas. This essay by no means devalues serious designs and plans, studies and research, ideas and claims revolving around cyber warfare. Rather, the purpose of this paper is to analyze existing jokes, hoaxes and hypes on the so-called cyber warfare, so as to distance serious research from misleading information.

Chapter XII is an article on regulation of cyberspace: Chinese law on cybersecurity and cybercrime. Since the advent of the network era, different countries adopted different stance on maintaining social order in cyberspace, either soft, strong, or in a medium of the way. In China, as in some other countries in the same group, a tough approach has been taken from the beginning. The purpose of this article is, by studying a series of legal actions against cybercrime, to explore into the Chinese model of regulation on cyberspace. In order to exercise control over the Internet, China has implemented statutory laws and administrative regulations revolving activity criminalizing, content filtering and user monitoring so as to maintain security and stability at both community and state levels. A tight legal and regulatory network has gradually weaved through recruitment of cyber police, investment on security technology, regulations on communications enterprises, and surveillance over users. Regardless of critics, this model was proved to have the merits of effectiveness in the specific socio-legal context in a short term.

Chapter XIII is an article on international actions against cybercrime: networking legal systems in the networked crime scene. This article reviews the international impetus of criminal law reform in combating cybercrime. This article classifies actions of international harmonization into professional, regional, multinational and global actions, summarizes the major concerns of these actions, and concludes the influence of the Convention on Cybercrime on state and international levels of legal countermeasure. The article also points out the limitations of the previous actions and anticipates the United Nations to play a more important role.

Helsinki, Finland, 6 June 2016

Xingan Li

TABLE OF CONTENTS

ACKNOWLEDGEMENTS.....	i
PREFACE.....	iii
CYBERSPACE AND THE INFORMED RATIONALITY OF LAW.....	1
EXPLORING INTO REGULATORY MODE FOR SOCIAL ORDER IN CYBESPACE.....	27
LEGAL-SERVICE-ORIENTED ARCHITECTURE.....	35
PHENOMENAL EXPLORATION INTO IMPACT OF ANONYMITY ON LAW.....	43
CYBERSECURITY AS A RELATIVE CONCEPT.....	65
THE CRIMINAL PHENOMENON ON THE INTERNET.....	79
E-MARKETING, UNSOLICITED COMMERCIAL E-MAIL, AND LEGAL SOLUTIONS.....	95
THE PHENOMENON OF UNSOLICITED E-MAILS WITH ATTACHMENTS.....	117
EXTENSION OF VICTIMIZATION IN UNSOLICITED E-MAIL MESSAGES.....	128
SPAM SOLUTIONS.....	157
CYBER WARFARE.....	168
REGULATION OF CYBERCRIME.....	181
INTERNATIONAL ACTIONS AGAINST CYBERCRIME.....	213

CYBERSPACE AND THE INFORMED RATIONALITY OF LAW^{*}

XINGAN LI **

ABSTRACT

Pervasive use of information system forms an irresistible force in shaping nearly all lives of our society. It poses great challenge to the previous legal system and requires special attention from the academic field. The purpose of this article is to identify potential change of legal systems in cyberspace, and to deal with the correlation between enhancement of legal literacy and the informed rationality. The article applies Weber's two-dimensional coordinate system comprised of "formality" and "rationality" and expands it into a three-dimensional model by distinguishing "informability" and "uninformability". The article also considers the relationship between internal and external control over the cyberspace order. Finally, the article discusses the infeasibility of the idea of computerized justice system.

Keywords: cyberspace, informed rationality, law, legal literacy, computerized justice system.

INTRODUCTION

Inventions and innovations during the last two or three centuries have revolutionized the landscape of human society, that has a recorded history of several millennia. Change, which could take a variety of styles, is not inevitably equivalent to advancement and improvement. Consequently, both constructive changes and unconstructive changes, both active and passive changes have been taking place where there are appropriate conditions and contexts. Pervasive dependence on computer information systems since the 1940s is one of such changes that utterly improves the general excellence of social life on one hand, but inexorably worsens certain aspects on the other. Contemporary society steps into an inconvertible position of deep addiction to this artificial instrument: while the

* Ideas in this paper were developed over years. An early version of this paper was published in Ahti Laitinen (ed.), *Writings in Sociology of Law and Criminology*, University of Turku, Finland, 2007. Subsequently, a revised and extended version was published in a collection of my articles, *Social Order in Cyberspace*, Amicus Law Books, Division, ICFAI University, India, 2009. Both books were in a small run and generally unavailable to external readers. This version, updated and revised, is to bring the ideas to a broader audience.

efficiency of production has been constantly enhanced, the foundation of conventional social control is challenged and shaken.

Information systems could hardly be considered as of either beneficiority or harmfulness according to an amalgamated criterion. Any criterion is unavailable due to the diversity of people's attitudes towards the value of overflowing information. The general public, nonetheless, have always been predisposed to pose it as a positive factor that assists interpersonal and international communication. The common use of "information systems" and of various other relevant terminologies, as a result, is, in a sense, any not neutral, but value-laden. It is as good as any spiritual and material asset. Some others also recognise the difficult issues in identifying the real value behind the surface of the illusory common knowledge about this new technological and social phenomenon: people connected through information systems might neither necessarily be as good as within a formally rational regime as Max Weber stated, nor necessarily be as bad as in "bellum omnium contra omnes" (Lat. the war of all against all) as in Hobbes' *Leviathan*¹, nor as ideal as in Plato's *Republic*, and Thomas More's *Utopia*. All the possible views are, however, in existence in defining the sphere of legal status of cyberspace.

This article will be devoted to identify the change, if not all improvements, of legal systems in the environment of information systems. It will first define the sphere of this discussion to exclude the so-called virtual space from cyberspace, pointing out that the virtual space, in the psychological and imaginary sense, is not relevant in addressing law. The article will be subsequently concentrated on issues of legal literacy. Information systems improve the enhancement of legal literacy on one hand; it posits the focus on informed rationality on the other. Formal rationality is one of the four ideal forms of law and legal thought constructed through Weber's two-dimensional coordinate system including "formality" and "rationality". (See Milovanovic, 1994, p. 40–47). The article depicts the revised model of Weber's ideal form of law and legal thought, by introducing Weber in a three-dimensional coordinate system. The article also considers the relationship between internal and external control over the cyberspace order. Finally, it discusses the infeasibility of the idea of computerized justice system.

¹ The Latin phrase itself was first presented in the preface of *De Cive* (Lat. *The Citizen*): "Ostendo primo conditionem hominum extra societatem civilem (quam conditionem appellare liceat statum naturae) aliam non esse quam bellum omnium contra omnes; atque in eo bello jus esse omnibus in omnia". (Hobbes, 1839, p. 148). I demonstrate in the first place, that the state of men without civil society (which state we may properly call the state of nature is nothing else but a mere warre of all against all; and in that warre all men have equall right unto all things.) The English translation is cited from a version printed by J. C. for R. Royston, at the Angel in Ivie-Lane, 1651 (available online at <http://www.constitution.org/th/decive00.htm>).

EXCLUSION OF CONCEPTUAL VIRTUAL SPACE

During the 1990s, there emerged many comments conceptualizing cyberspace as an unadulterated and uncontaminated “virtual space” (Mason, 1998), without any involvement of people, society and state. Neither would cyberspace invade and infringe society, nor would society invade and infringe cyberspace. Under such a perspective, cyberspace could be explained as a space mirage existing in information-systems-facilitated games, communications and germane economic transactions. The most noteworthy instances were those where “virtual rape” was perceived by a number of authors to be committed (Dibbell, 1993) and losses of virtual property were undergone (The concept of virtual property has been defined in various ways, particularly in articles written by different authors representing various disciplines; for a few examples, see Bartle, 2004; Fairfield, 2005) by cyber game role-players. Under such circumstances, I understand that a virtual space is an imaginary space (not necessarily a place) where real human individuals exist and behave behind a curtain of sign, symbol, or graphic-being represented by bits and bytes of digits. Virtual rape is not a human physical experience but one during which a feminine sign, symbol, or graphic-being manoeuvred by a human player (not necessarily a female) is subject to a position of similar psychological and imaginary suffering through activities performed by a masculine sign, symbol, or graphic-being manoeuvred by another human player (not necessarily a male). Thus far virtual rape is not rape in the legal sense, even to the dawn of the information age.

A virtual property is a sign, symbol, or a graphic-being available with the cost of real money, that is, it has use value and exchange value and is a commodity, even though it exists only within the sphere of information systems.

While we are barely convinced to accept a case where virtual rape is comparable to real rape and subject it to the criminal justice system, we are prone to confirm the status of virtual property as real property, because it has the same attributes as that of a real property: exchangeability through the intermediary of money.

Once “virtual property” enters the sphere of circulation through the intermediary of money, be it a sign, a symbol, or a graphic-being, it becomes a thing that we are measuring through such a ruler as value. It does no longer stand still in a pure psychological and imaginary sphere as ambiguous as virtual rape. It comes out of virtual space and goes into real life. If we own this “virtual” property valued one million dollars, we are millionaires through the value of this sign, symbol, or the graphic-being. If burglars or robbers take this “virtual property” away from us, we are suffering loss. It is now no longer “virtual” at all.

When we explore law in cyberspace, we are not discussing about anything that is so unperceivable as virtual rape, or virtual space. Rather, cyberspace is simply an extension of the real space, of our society. It is the extension of this society through the facilitation of information systems that connect many people

in different temporal and spatial distributions into globally accessible, 24/7/365 available, and linguistically-interpretation-powerful networks. Society has been a web, but this is a new style social web with intervening factors of machine filling situated in the human-human interaction process. The new social web is constructed more by instant and remote chains of human-machine-human interactions. The quantity of face-to-face human-human interactions decreases and its role weakens.

The social order along the newly-emerged social ties, however, would not be expected to turn over the fundamental social order. Rather, the conventional social order would be to operate continuously with the assistance of machine-enabled mechanisms. People, societies and states should not enter a cave or hole as virtual as a psychological and imaginary space and begin their exploration into the value of existence from the beginning of history. Law and order would become more realistic and simplified if our conventional mechanisms run in the same to operable way as in the past. Cyberspace thus gives more sense to the extent that its existence empowers the existing social order, regardless of its reasonable or unreasonable character. In sum, the creation of cyberspace extends the sphere of existing society, but does not carry the function of undermining the current society or separating it from its traditional frame.

IMPROVEMENT OF LEGAL LITERACY

Although cyberspace would not be as bizarre as a society that is as virtual as a psychological and imaginary phenomenon, it would bring about changes relevant for the present status of society. Cyberspace is a new field and a new frontier that runs law and order of our society as a programme. It does more than merely copying, duplicating or repeating conventional modes of law forms and legal thought.

The quality of the legal framework and the effect of its operation are severely dependent on the legal literacy of citizens. Traditionally, legal illiteracy is not even a reason for citizens to be more or less excused, because there is such legal maxim as “*ignorantia juris non excusat*” (No one should be excused for his ignorance of the law). Here, by legal literacy, we refer to the condition of people knowing law and thus becoming subject to the order under the constraint of law.

As far as legal literacy is concerned, the degrees to which literacy exists differ from one person to another. There are persons (citizens) who are rather legally illiterate, persons who are more or less legally literate, and others who are highly legally literate. Certainly, there is hardly one who is absolutely legally illiterate and one who is completely legally literate. Literacy exists on one certain point along the line of degrees between zero percent and one hundred percent. Thus far, we can list ideal types of citizens according to different degrees of their legal literacy:

1. those who are illiterate and are also legally illiterate of both domestic law and foreign law;
2. those who are literate but are legally illiterate of both domestic law and foreign law;
3. those who are literate and are also legally literate of domestic law but not of foreign law;
4. those who are literate and are also legally literate of foreign law but not of domestic law;
5. those who are literate and are also legally literate of both domestic law and foreign law.

The reasons why citizens are illiterate of law are many, but two of them are of utmost significance: the unawareness of citizens and the unavailability of law.

The unawareness of law was once a primary factor for citizens to hold an alienate attitude towards any law, be it of civil or criminal nature. In many countries in previous centuries, ties with something called “law” were somewhat bad, unfortunate or pertaining to mystery. Therefore, persons who were assigned as subjects operating law would be mystified as a result of their priority over power and knowledge, through such symbolic things as crosiers and ritualistic robes; persons who were involved in legal issues would be categorized as either vulnerable individuals who suffered from infringement or invasion from others, or vulgar individuals who imposed infringement or invasion on others. As a whole, law has not been a usual practise in daily life and social activities. On the contrary, escaping from law and relevant affairs was preferred by the majority of citizens.

The awareness of law has been increasingly strengthened over years due to the seriousness and severity of legal issues being decreased and the position of the legal profession being demystified. The current situation is that even though no one knows everything about law, most citizens know something about law. The legal profession is gradually becoming a profession that is increasingly comparable with other specialities, in Durkheim’s words, different divisions of labour in society. Therefore, unawareness of law is gradually becoming a minor reason for citizens’ legal illiteracy.

The other important reason for which citizens are legally illiterate is the unavailability of law. In ancient times, the universal practise was that “if the penalty remains unknown to all, its power would be immeasurable.” (The words are cited from the comments by Kong Yingda, a Chinese writer in Tang Dynasty on a classic *Zuozhuan* in the volume of *Zhaogong*.) The function of earlier law was supposedly repressive (See Durkheim, 1933.) With the view to maintain the repressive ruling order, the ruling class needed to grasp, control, monopoly and manoeuvre the legal power. Along with the change of the legal function, the “keeping-unknown” of law became less important in maintaining the mysterious power of the state. Thus this issue became less significant in unavailability of law. The notion was only one side of the coin of the the unavailability of law that kept

law far from the reach of citizens. The other side of the coin was that the specific conditions of transportation and communication in the ancient times made it impossible to inform most population about law.

Thus, the active refusal of law on one hand, and the passive refusal of law on the other, severely impeded the wide spreading of legal bodies, legal knowledge and legal consciousness. The coming of the legal enlightenment did not happen until the end of the Middle Ages. Thomas Paine stated the principle of rule of law in 1776: "For as in absolute governments the king is law, so in free countries the law ought to be king; and there ought to be no other" (Paine, 1844, p. 28).

In modern times, it is not true that citizens are legally well informed. Even today, states are not fully making efforts to inform their citizens about law. However, there is an interfering element in spreading law: the invention of the electronic digital computer and the connection of information systems through the publicly-accessible networks. Once the printing technique and wide-distributed libraries made it possible that every citizen could access available bodies of law. However, availability of law depends on the limits of time and space. Contemporary information systems change the picture of legal availability and accessibility by providing the possibility of superseding the spatial-temporal boundary of looking up a printed copy.

Other facilities and inventions did ever improve the availability of law – we have in view the postal system, telephone, telegraphy, and facsimile. But the severe dependence on human resources and the high expenses implied still left it unreachable to most of the population. Current information systems seemingly overcome the shortcomings of traditional media.

However, we must bear in mind that getting informed about law (or medicine, or doing many other scientific practices) is not like doing dictionary looking-up. What we view, read and understand does not equal what we would receive by reading from specialised legal agencies. Therefore, specialised legal agencies are not substitutable through the common reading of law and widespread legal knowledge. Society should aim at giving its citizens the chance of a better access to law and legal knowledge, so that they could achieve a higher level of legal consciousness. The evolution will help to demystify the legal bodies and the legal profession, to maintain legal rights and limit the arbitrary power.

INFORMED RATIONALITY

When Weber proposed his ideal models of law forms in *Economy and Society*, he had hardly the concern about whether citizens were legally informed or not. Therefore, we could imagine Weber as depicting his models on the premise of

citizens being either completely legally informed or completely legally uninformed. But today, we are confronted with an increasingly deep concern about the issue whether citizens are legally literate or informed, because we are in an age when people are better informable due to tremendous information systems, and they are migratable, due to the powerful transportation mechanisms.

If we could suppose that the ideal model of form of law in the past consisted of uninformed formal or substantive rationality or irrationality, then our model thereafter should be revised as informed formal (or substantive) rationality (or irrationality). Thus we could place Weber's ideal models into a 3-Dimensional coordinate system. Borrowing from Weber's four ideal forms of law and legal thought, plus our extra dimension of informability, then we have (the description part of each item mainly refers to the induction of Milovanovic, 1994, while the part about informability is my own):

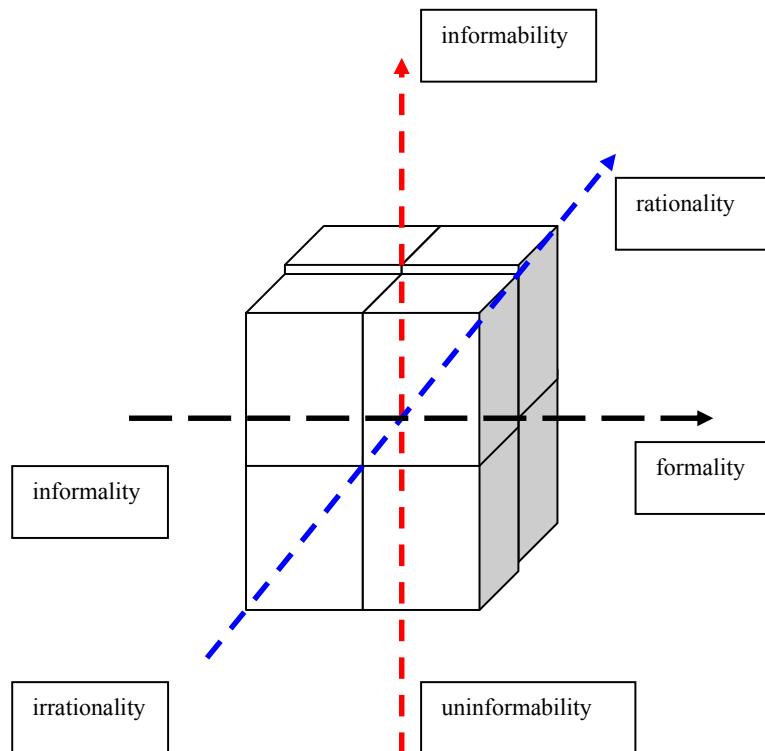


Figure 1. Three-dimensional coordinate system of forms of law and legal thought.

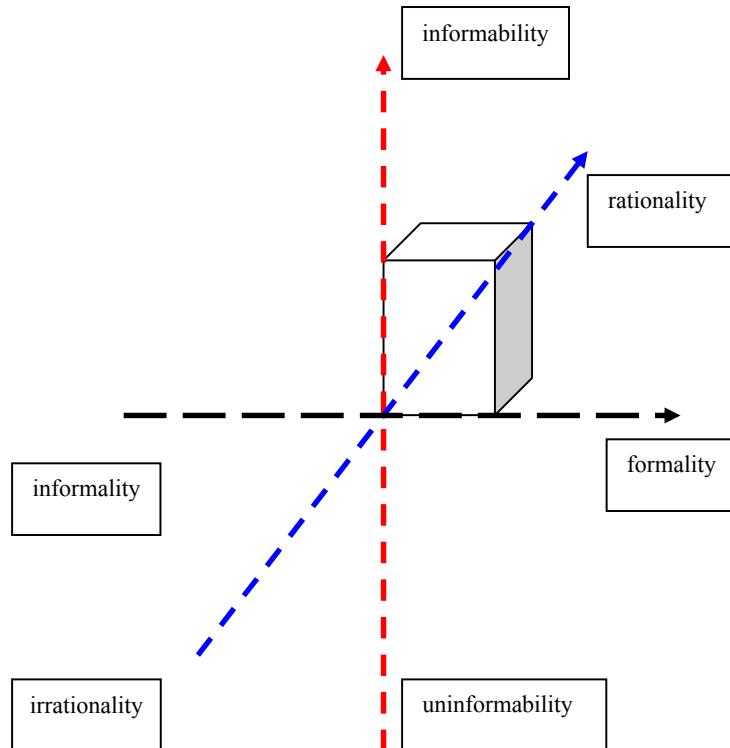


Figure 2. Informed formal rationality.

Informed formal rationality. This represents formal rationality with the subjects informed. Under this model, the legal system was operated under the circumstances where clearly-addressed and clearly-observed rules were applied to all like cases in a consistent form. Similarly situated were similarly treated, without external interference with the decision-making process. Besides, the decision-making process has a higher degree of transparency by ensuring that the subjects are informed about the applicable rules and/or processes. In sum, this model could be trichotomized as unified criterion, due process, and transparent operation.

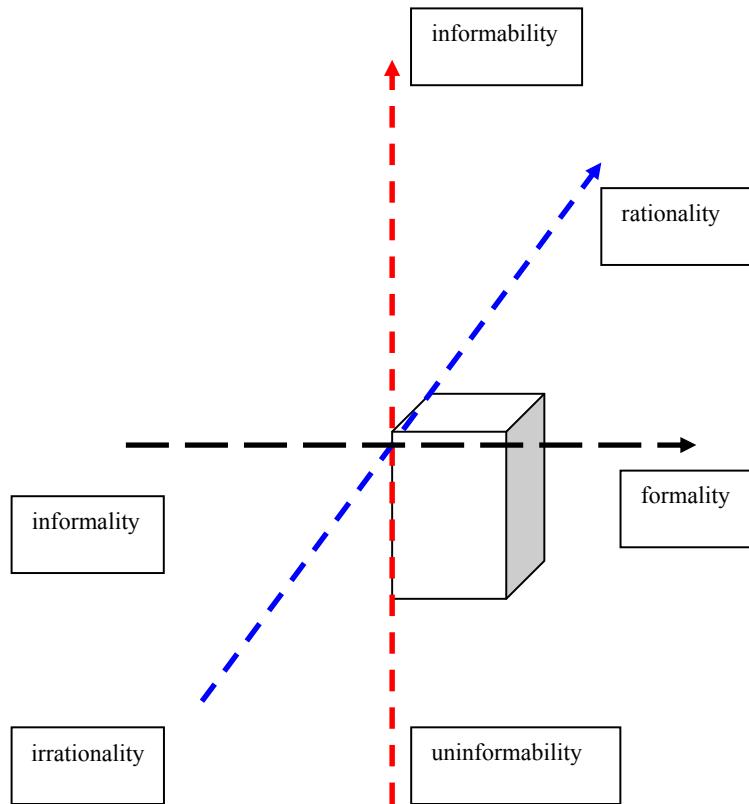


Figure 3. Uninformed formal rationality.

Uninformed formal rationality. It represents formal rationality without the subjects informed. Under this model, the legal system was operated under the circumstances where clearly addressed and observed rules were applied to all as cases in a consistent form. Similarly situated were similarly treated, without external interference with the decision-making process. However, the decision-making process has a relatively low degree of transparency and the subjects are not informed about the applicable rules and/or processes. In sum, this model could be trichotomized as unified criterion, due process, and opaque operation.

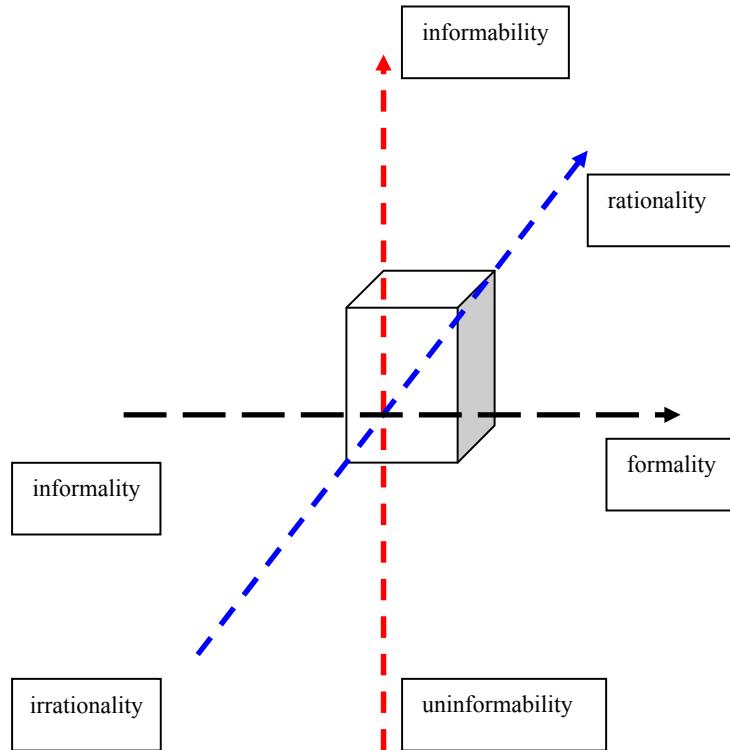


Figure 4. Informed formal irrationality.

Informed formal irrationality. It refers to formal irrationality with the subjects informed. Under this model, the legal system was operated in the process where it was uncertain whether clearly addressed and observed rules were applied to all similar cases in a consistent form. Similarly situated were differently treated, with some mysteriously arranged mechanisms functioning in the decision-making process. Arguably, the decision-making process has a certain degree of transparency by providing opportunities for the subjects to be informed about the applicable rules and/or processes. In sum, this model could be trichotomized as diversified criterion, due process, and transparent operation.

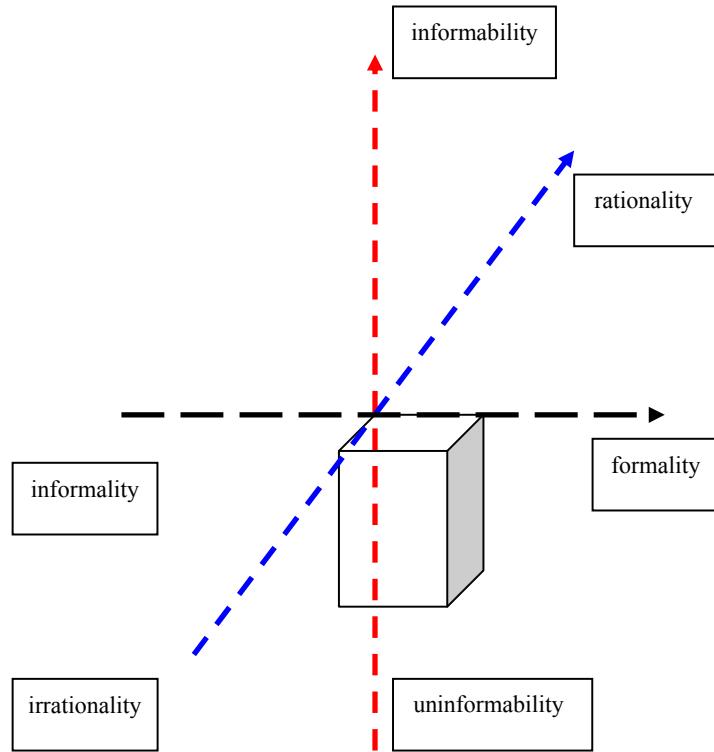


Figure 5. Uninformed formal irrationality.

Uninformed formal irrationality. It refers to formal irrationality without the subjects informed. Under this model, the legal system was operated in the process when it was uncertain whether clearly addressed and observed rules were applied to all like cases in a consistent form. Similarly situated were differently treated, with some mysteriously arranged mechanisms functioning in the decision-making process. The decision-making process was absolutely secret through depriving any degree of transparency by denying opportunities for the subjects to be informed about the applicable rules and/or processes. In sum, this model could be trichotomized as unified criterion, due process, and opaque operation.

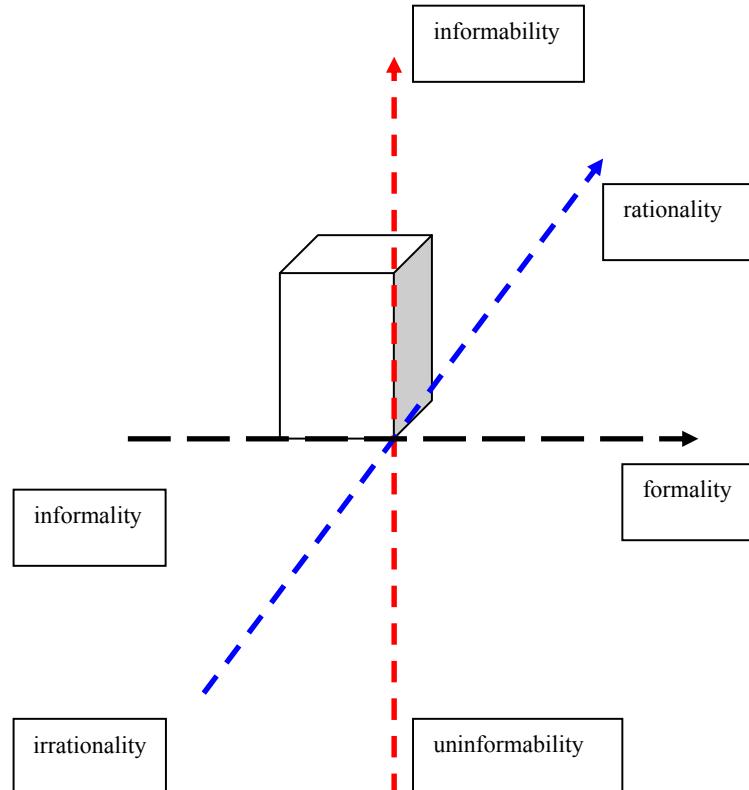


Figure 6. Informed substantive rationality.

Informed substantive rationality. This model implies substantive rationality with the subjects informed. Under this model, the legal system was operated under the circumstances where clearly addressed and observed rules were applied to cases according to the detailed situation. Similarly situated were differently treated, with severe external interference with the decision-making process. Besides, the decision-making process has a certain degree of transparency by providing opportunities for the subjects to be informed of the applicable rules and/or processes. In sum, this model could be trichotomized as diversified criterion, random process, and transparent operation.

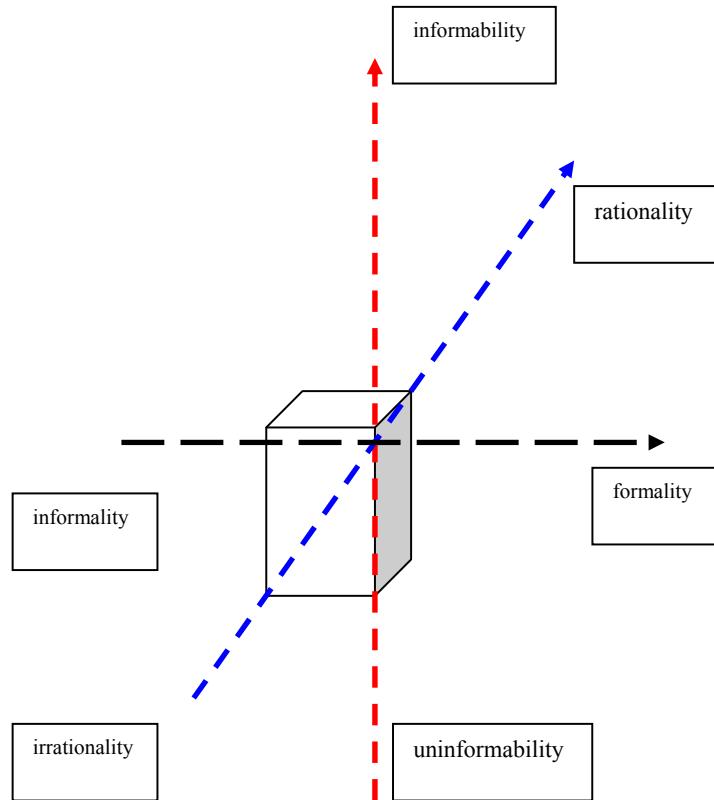


Figure 7. Uninformed substantive rationality.

Uninformed substantive rationality. This represents substantive rationality without the subjects informed. Under this model, the legal system was operated under the circumstances where clearly addressed and observed rules were applied to cases according to the detailed situation. Similarly situated were differently treated, with severe external interference with the decision-making process. Furthermore, the decision-making process has no transparency due to denying opportunities for the subjects to be informed about the applicable rules and/or processes. In sum, this model could be trichotomized as diversified criterion, random process, and opaque operation.

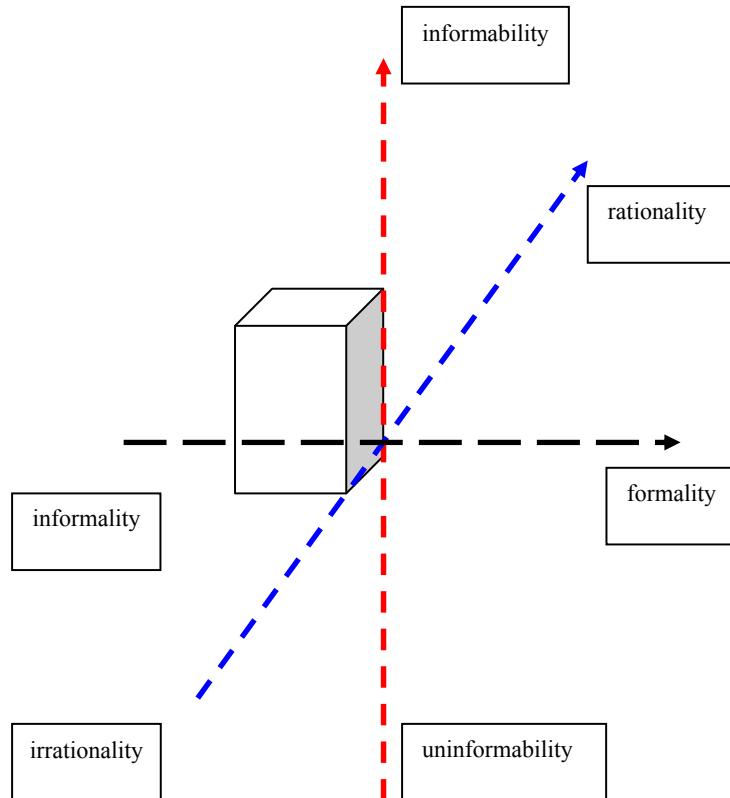


Figure 8. Informed substantive irrationality.

Informed substantive irrationality. It shows substantive irrationality with the subjects informed. Under this model, the legal system was operated in the process when detailed situation determined the decision. Similarly situated were differently treated, with severe external interference with the decision-making process. Ironically, the decision-making process has a certain degree of transparency by providing opportunities for the subjects to be informed about the applicable rules and/or processes. In sum, this model could be trichotomized as diversified criterion, random process, and transparent operation.

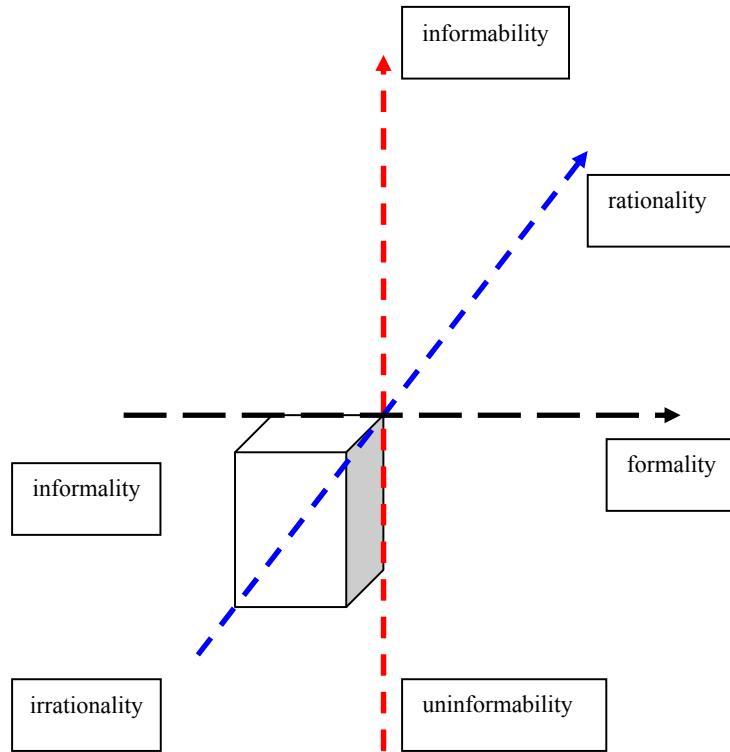


Figure 9. Uninformed substantive irrationality.

Uninformed substantive irrationality. It refers to substantive irrationality without the subjects informed. Under this model, the legal system was operated in the process when detailed situation determined the decision. Similarly situated were differently treated, with severe external interference with the decision-making process. Furthermore, the decision-making process has no transparency due to denying opportunities for the subjects to be informed about the applicable rules and/or processes. In sum, this model could be trichotomized as diversified criterion, random process, and opaque operation.

In the past, the legal form of law sank under the surface drawn between the informed and the uninformed. That is to say, it was located in a certain point within the contour constituted by the points of Uninformability-Informality-Irrationality-Formality-Rationality. Today, it has been raised to the level of being informed. Thus we are talking primarily about the informed form of formal (or informal) rationality (or irrationality), located within the contour constituted by the points of Informability-Informality-Irrationality-Formality-Rationality. That is the upper part of the coordinate system, which is floating above the surface by information systems.

LIMITED CHALLENGE TO THE CONVENTIONAL STATUS OF LEGAL PROFESSION MONOPOLY

In the past, legal profession happened to be highly monopolistic, mainly through the close control of the texts of law: everyone who wanted to know law was denied the chance to know, with the exceptions of those situations when the legal agencies publicized law through some limited fixed form (for example, ancient Romans' *The Twelve Tables*). The legal system was manoeuvred by a group of people who were not necessarily the representatives of citizens and who operated secretly and mysteriously.

The legal profession grew less and less monopolistic due to the evolution of society in general and to the transparency of the legal system in particular. But without citizens being well informed of law, it remained highly secret, mysterious and monopolistic: everyone who wanted to know law was neither denied nor granted the chance, but remained unable to know more.

Rendering public the real face of law has never been fully ensured throughout history. But with citizens highly informed, the monopoly of legal profession is confronted with a strong challenge: everyone who wants to know law is not denied but granted the chance, and is really able to know. The going-online of laws and governance into information systems and the development of the legal retrieval system serves both legal professionals and citizen laymen of access to law. The monopoly of legal profession through control of legal texts becomes uneasy.

The development, however, does not represent a process of breaking up the monopoly of the legal profession in a foreseeable future. Rather, the monopoly is achieved more through control of employment quota and qualification but less through control of bodies of law. This is related to a more important and more complicated issue in which the achievement of the qualification for legal profession could only be possible through the specialised legal training during which only a limited number of people could be taught the legal discourse, which others could hardly grasp through merely reading the clauses of law. Anyway, information systems do not provide systematic law school education. Even if they do, it is still different from what the officially qualified legal professionals received in the original form of law school. The legal profession is thus determined to be monopolistic, despite that the monopoly of legal texts is less strong than before, when there was not any legal retrieval system. In a word, the resistance of the conventional sets of factors of the legal system is not sensitive and vulnerable to the upcoming new challenge.

PRIMITIVE CYBER SOCIETY

Another dimension we are concerned with is related to the legal order in cyberspace. We could find little evidence on whether the cyber society will repeat or replicate the developmental process of the traditional or non-cyber-society. But we have witnessed a lot of statements that impressed us as if they described the state of the emerging societal existence in relation with information systems as in a primitive stage depicted by writers only in the last several centuries. While whether what they have actually experienced or investigated were “primitive” societies is still to be determined, we could find a publicly recognized model of primitive society characterized by lower developed culture, economy and political structure. The similar situation occurred in the inquiry of the cyber society and an impression of primitive cyber society is quite clear in current literature.

Hobbes’ Leviathan, and Rousseau’s state of nature were relatively pessimistic scenarios. Marxian primitive communist society was a far more optimistic picture than theirs. In this primitive communist society, there was no private property, no class and class struggle, no state, no deprivations. People commonly owned both productive and living materials, commonly worked and lived, and equally distributed products. Only when private property, the source of all evils, emerged did the primitive society become involved into conflicts of interests. Despite all these distinctions between the viewpoints on how the primitive society existed, the twentieth century observers from different standpoints viewed the emerging cyber society as different from those primitive societies observed several centuries ago.

Classic writers wrote on the primitive societies from relatively *post de facto* positions, while the modern writer writes about the primitive cyber society from relatively *priori de facto* positions. It could be safely said that the classical writers hardly ever lived a practical life in the primitive societies they investigated, heard, wrote or imagined. At best they were observers of some of the objects, but their observations were not sufficiently convincing evidence to prove us that these objects were the just models that preceded societies of ours, or more exactly, of the classical writers who were inquiring. In fact, the practical primitive societies of the current mainstream societies remain unknown to present people. Cyber society, however, has been closely witnessed by many of the commentators who write about its developmental process. Therefore, the primitive cyber society might be one of the primitive societies that have ever been mostly investigated and written, if there was ever another one that was investigated and written by writers in person.

INTERNAL AND EXTERNAL CONTROL OF CYBER SOCIETY

Control over a society can be mobilised by either internal or external factors, or in case there is no control at all, by neither internal nor external factors. But it is a rare case where there is no control, or no order at all. However, most writers are claiming that the cyber society is not regulation-free, because order exists everywhere maintained by certain internal or external control mechanisms.

Society could be regarded as representing integrity, of which cyberspace is a part. The order of cyberspace is also a part of the integrative order of society. Cyberspace as a social existence, however, has special patterns and could be defined as a sub-societal unit. The order maintenance in cyberspace, therefore, could be achieved by internal control and/or external control (for society as a whole, it is still internal control).

Those concerned with the organizational forms of cyber society only wrote about what they observed and found. To understand the full picture of the complicated situation of the possible organizational forms of a society, we should use the ideal models of the internal and external control in order to simplify observations and descriptions of it.

Order can be maintained in different degrees and by either internal or external mechanisms. The internal control is the order maintenance through the internal mechanisms within the cyberspace. That is to say, the netizens self-regulate themselves by adopting codes of practice. The internal control is characterized by three considerations: **1.** the netizens in the cyberspace could not engage in legislation activities and implement forcibly enacted rules such as constitution or law, but could only compile ethical codes with sanctions limited to the change and refusal of services; **2.** cyberspace is a place where inheriting inequality prevails and netizens are situated in an unequal status due to their inequality existent before they migrated into the cyberspace; **3.** once established, the internal control has little influence on the external control, but external control has a strong impact on internal control. Based on these characteristics, the decision-making process of the code of practice for the internal control is hardly run with the principle of democracy and mass participation. Rather, these codes are simply drafted by one or two persons who have more concern with their commercial benefits from the service provision, with limited reference to the reaction and comments from the service users. The discretion is at the side of the service providers on the scale.

The external control is the maintenance of order through external mechanisms outside the cyberspace. The pure external control refers to law and order being solely imposed by the state. There cannot exist such external control with the source of power coming from any other organs. When we consider the issue of external control, therefore, we are inevitable to place netizens into the web of real society, which could in no way escape from the constraint of law and regulation.

By referring to internal and external control, we temporarily separate the cyberspace that does not exist without the connection of information systems, from the meat space, that is, society that has existed without information systems but has integrated information systems into its territory. More safely speaking, the frontier between cyberspace and society in the broader sense is only drawn for the convenience of this theoretical framework. Otherwise, I am strongly insisting that the cyberspace should be regarded more as an extension and an integral part of society. What information systems connect are the elements of this society, but the elements of this society do not become independent and connected in a space of their own.

The possible forms of incorporation of internal and external mechanisms could be induced as the following:

1. ABSENCE OF INTERNAL CONTROL, ABSENCE OF EXTERNAL CONTROL

This is a case where neither internal nor external power was installed to operate deliberate control over the order of the cyberspace. It is a rare case with little or no internal or external factor directly controlling over the cyberspace. But there exist arguments that claimed to leave the cyberspace maintained by pure technological mechanisms. This is a kind of preset arrangement, with human factors appearing far behind the appearance of their codes and programs.

Rather than case-by-case judgment over activities in the cyberspace according to existing rules, order is maintained by preset rules that only deal with a variety of situations through mechanical application of unified standard. In sum, this is a kind of technological control, with instant internal or external human elements being absent. The model could be depicted as in the following figure:

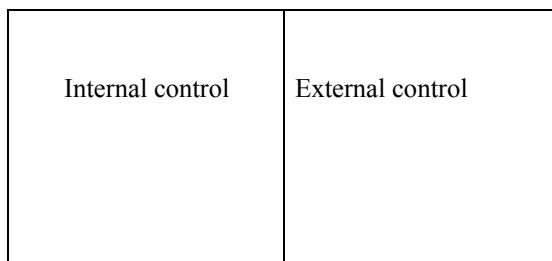


Figure 10. Absence of internal control, absence of external control.

Under this model, the cyberspace was in a state of anarchy (anarchy does not necessarily mean confusion). The advocates of anarchic cyberspace claimed that the cyberspace has been created solely by technicians with technology, in a way which is independent of society, and free from the governing of the state while forming a new existing space. This is a kind of space where the human relationships are in the “null-gravity state”. We can well describe it as the balance

in the unbalance, the order in the disorder. The activities under such circumstances involve lower costs but take higher risks. Without any regulation and control, the Wild West metaphor of the virtual community will be the most appropriate. (Many authors have exploited the metaphor of “Wild West” about the circumstance of the cyberspace. For random examples, see Morris, 1998; Clairmont, 1998, p. E1 and E2.)

Due to the vacuum structure of this kind of cyberspace, the occurrence of collapse and disruption would be inevitable sooner or later. Thereafter, the attempt of internal control, motivated by desire of ownership of interests and dominative power, and/or external control, motivated by maintaining and enlarging existing interests and power, would take place. It is therefore an instable and unacceptable structure.

2. ABSENCE OF INTERNAL CONTROL, PRESENCE OF EXTERNAL CONTROL

Under this model, the internal control mechanism is not established. The order maintenance is primarily the task of the extended control from society as a whole. Although society might have different degree of democracy or autocracy, and it would naturally extend the existing mechanisms into the cyberspace, for the cyberspace, an autocracy was created with the absolute and exclusive external control, without a position of internal control, that is, through the participation of the Internet users.

This autocracy is not an autocracy in its true sense, where a society is controlled by a few people who arbitrarily exercise control over the majority. Here, the cyber autocracy was only under the pressure from outside the cyberspace, lacking any internal control mechanism.

In addition, autocracy is not one fixed model. Rather than an absolute form of autocracy, its possible forms might differ from each other by the degrees of autocratic nature. At the same time, cyberspace differs from society as a whole according to the degree in which control power is enjoyed.



Figure 11. Absence of internal control, presence of external control.

If netizens enjoy few rights to organize themselves, and the government maintains the order solely, the cyberspace could be subject to a higher degree of autocracy, and vice versa. The current situation is that the government polices the cyberspace in the same way as the traditional society. The rate of the cyberpolicemen to the whole population of netizens is close to, or higher than the rate of the policemen

to the whole national population. Therefore, the cyberspace might become a special zone of society but could not remain syncretised with the social unity.

Under such a model, the cyberspace is disciplined forcibly by the external power. For society as a whole, the activities would involve higher costs but take lower risks. However, the external control might meet with resistance from the netizens in the organized form. Again, the external control might not completely fulfil the requirements of the running of the cyberspace, which is in a sense like a well built machine. Stepping into the stage of the internal control would thus be unavoidable.

3. PRESENCE OF INTERNAL CONTROL, ABSENCE OF EXTERNAL CONTROL

This mode of cyberspace is organized according to the common ethics established within the online community. While ethics is needed, law is lacking. On one hand, it is not possible to implement rules on the level of “law” due to the absence of the legislative power and institutions. The available and feasible rules fall on the level of ethical dimension.

On the other hand, ethical dimension is relatively developed in cyberspace due to the initial independent development and self-regulation practice. The advocates of the mode believe that the ethical mechanism can work well, thus keeping the cyberspace into order. The netizens under this model constraint their own behaviours according to the ethical code of the cyberspace, abstaining from the breach of the cyberspace, and from invading society. However, the internal control might be confronted with the risk of breakdown due to lack of forcible enactment of sanctions, thus calling for the outside interference, that is, the filling-in of the external control.

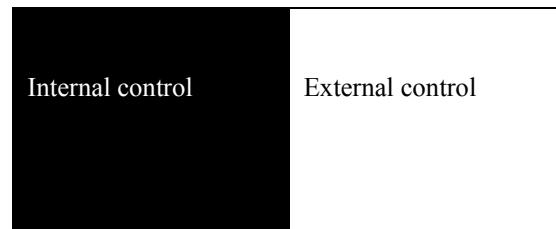


Figure 12. Presence of internal control, absence of external control.

4. PRESENCE OF INTERNAL CONTROL, PRESENCE OF EXTERNAL CONTROL

By the fourth model, we are seeking to balance between the external control and the internal control. Both controls would play roles in the order-maintaining process. This includes balance between internal factors, between external factors, and between internal and external factors. The model includes both a certain degree of internal control and a certain degree of external control, in which the activities might involve higher costs but take medium risks.

The creation of this dual control could either be the result of compromise between the desires of cyberspace as an integral part and as an autonomous zone of society as a whole on one hand, and the other parts of society; or be a result of conspiracy between some of the netizens and the other part of society. Regardless of the nature of such compromise or conspiracy, despite the continuous change of balance between powers of internal control and external control, this is the most possible and stable model, be it not within the ideals of many acclamations.

The leverage in this model could move from the left to the right, that is to say, the degrees of internal control and external control could differ from strong and weak. In some case, as depicted in *Figure 13 (1)*, the internal control is weaker but the external control is stronger with the leverage located in the left part deep into the frontier of the internal control. In *Figure 13 (2)*, the internal control and the external control are ideally balanced with the leverage located on the medium frontier between internal control and external control. In *Figure 13 (3)*, the internal control is stronger but the external control is weaker with the leverage located in the right part deep into the frontier of the external control.

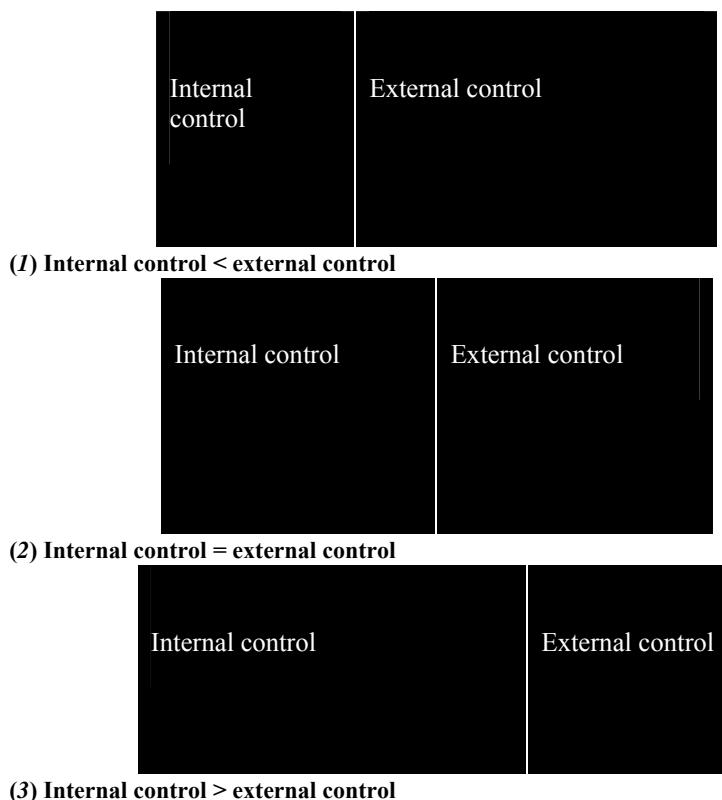


Figure 13. Presence of internal control, presence of external control.

We can hardly conclude which model is the beneficial or practical. It is a question of which discourse is the dominant. There are those who advocated the cyber anarchy, leaving the cyberspace as it is, resisting any artificial control either from inside or from outside. Yet their voices have been too weak to be heard by the netizens and non-netizens. Particularly, society's prevalent discourse might not be compatible with an anarchist view. The same happens in the cyberspace. Many also argued for solely internal control over the cyberspace, denying the externally imposed state arrangement. However, in this case, it is not words, grammar and reasoning that are functioning. It is the legislature, police, court and jail doing so. Therefore, solely external control rather than solely internal control is more proximate to the goal of the order of the social unity.

Given neither absolute internal control nor absolute external control is possible, the more acceptable and more stable structure of cyberspace order might be under a mechanism in which the cocktail of internal control and external control is mixed. It is as if the cyberspace were a globe, inside which the force of gravity attracts the elements and materials towards the core, while the outside pressure condenses its cubage. As a result, cyberspace exists in the shape of a dwarf star, only in which form, cyberspace becomes an integral part of society as a whole, with a stable and acceptable order.

THE RISK OF THE HYPOTHESIS OF FORMAL RATIONALITY TOGETHER WITH COMPUTERIZED JUSTICE SYSTEM

Modernity of law was supported by many idealistic ideas of which formal rationality is one most recommended by the Enlightenment thinkers, but one most criticised by the postmodernist advocates. The ideal of formal rationality believed that rule of law could be achieved, given goals such as systematization of legal system, installation of professional jurists, well arranged processes etc.

The use of the powerful computing machine in the latter part of the last century became an incentive for those who insisted that formal rationality could be achieved with the help of the mechanical calculation of the elements of mens rea, actus reus, due process, equal protection, etc. Their inevitable operations have been to quantify both the quantitative and the qualitative factors with the tools of pinch cards, sentencing guidelines and computer software.

Ironically, the coming of the idea of computerized justice system roughly coincided with the initiation of the postmodernist criticism against the blankness of formal rationality. The phenomenon could well be conceived as a hidden form of resistance of the despairing ideal of rule of law against the possible adaptation to the changed social environment. While legal retrieval system is a beneficial element in impelling subjects to be more informed about the certainty of the law, the computerized justice system might pose a hindrance by maintaining the conventional order on the contrary direction to the former.

In all accounts, mechanical computerized justice system is not akin to the postmodernist legal studies. It is a misplantation if there is such a discourse as to incorporate such different creatures in the macro-environment where what happened simultaneously is prone to be considered to have the same features. In doing such logic reasoning, the balance of linguistic powers out of the opposed fronts is inevitable and unfortunate.

The use and abuse of information systems in doing law and legal studies are common occurrences in current time. But the divarication of the use and abuse would come into being sooner or later. This would imply giving up the seemingly reasonable but practically unreasonable ideas, divulged from the prevailing information systems facilitating legal discourse. Thus the clarification of the role of the mechanical computerized justice system and the like should be given first priority in addressing the informed legal order of society and its extension into cyberspace. The time when everything could be hidden behind this information curtain and appear with this fashioned mask would come to an end, together with the dream of mechanical computerized justice system. Information systems, in fact, cannot do such a thing as doing law. The basic questions such as "who would write codes and compile law into such a program?" and "who would sit at the desk to finger keyboard to operate such a system?" cannot even get logic answers without referring to the outdated ideals.

CONCLUSION

The change of legal systems in the environment where the pervasive use of information systems forms an irresistible force in shaping nearly all lives of society needs specific attention. The discussion above briefly defined the limit of its boundary. While we have the very reason to exclude the so-called virtual space from the current field, we make no attempt to negate the value of further inquiry into all the unique respects brought about by the development and understanding of the new technologies, which in turn indeed leads the old legal thinking up to a novel platform. It is on this higher level that the hypotheses of improved legal literacy and informed rationality operate. The other objectives of this essay are to construct the models of order in cyberspace over which internal and external forces exercise control to varying degrees. Although the information society in general and the cyberspace in particular are designed toward an environment accommodating a more ideal legal system, mechanistic calculable justice standard would not be realizable in an optimistic future.

REFERENCES

1. BARTLE, RICHARD A. (2004). *Pitfall of Virtual Property*. Retrieved 14 January 2009, from <http://www.themis-group.com/uploads/Pitfalls%20of%20virtual%20property.pdf>
2. CLAIRMONT, SUSAN (1998). Police Compare Cyberspace to the Wild West and Dangerous, in *The Hamilton Spectator*, 14 August, p. E1 and E2.
3. DIBBELL, JULIAN (1993). A Rape in Cyberspace, in *Village Voice*, Volume 38, Number 51, 12 December. Retrieved 14 January 2009, from <http://www.ludd.luth.se/mud/aber/articles/village.voice.html>
4. DURKHEIM, EMILE (1933). *The Division of Labour in Society*. Glencoe: The Free Press.
5. FAIRFIELD, J. (2005). *Virtual Property*, Boston University Law review, Volume 85, p. 1047–1102.
6. HOBBES, THOMÆ. *Malmesburiensis opera philosophica quæ latine scripsit omnia*, Vol. II, Londini: Apud Joannem Bohn, 1839.
7. HOBBES, THOMAS (1962). *Leviathan*, New York: Collier.
8. MASON, MOYA K. (ed.) (1998). Bibliography, in Howard Rheingold, *The Virtual Community*, 2nd Edition. Retrieved 14 January 2009, from <http://www.rheingold.com/vc/book/biblio.html>
9. MILOVANOVIC, DRAGAN (1994). *A Primer in the Sociology of Law*, 2nd edition, New York: Harrow and Heston Publishers, p. 40–47.
10. MORE, THOMAS (1989). *Utopia*, Cambridge: Cambridge University Press.
11. MORRIS, ANDREW P. (1998). Feature: The Wild West Meets Cyberspace, in *The Freeman: Ideas on Liberty*, Volume 48, Number 7.
12. PAINE, THOMAS (1844). *Common Sense*, Dedham, Mass., re-printed by H. Mann for S. Bryant, esq.
13. PLATO. *The Republic*. Retrieved 14 January 2009, from <http://www.gutenberg.org/dirs/etext94/repub13.txt>
14. *The Twelve Tables*. Retrieved 14 January 2009, from <http://www.fordham.edu/HALSALL/ancient/12tables.html>
15. WEBER, MAX (1978). *Economy and Society: An Outline of Interpretive Sociology*, Guenther Roth and Claus Wittich (eds.), Berkeley: University of California Press.

Exploring into regulatory mode for social order in cyberspace

Xingan Li

LLD, PhD, Associate Professor, Tallinn University Law School, Narva 29, 10120 Tallinn, Estonia.
E-mail: xingan.li (at) yahoo.com

Received October 26, 2014; Accepted December 22, 2014

Abstract

An increasing necessity for building social order in cyberspace through legal instruments has existed as one of many alternatives to regulate the world dominated by the globally connected Internet. This article discusses legal gaps of cyber-laws among different localities, with special regards to regulation over Internet content, through an approach with emphasis on players in three different steps of data movement that are separately characterized by human-machine, machine-machine and machine-human interaction with different degrees of human intervention. From the features of each stage, it is concluded that official action must be within the ability of the controller so that it can be effective, and that it must also cope with the utility of the controller so that it can be efficient, so that an ability-and-utility-oriented control mode would ideally functions.

Keywords

Social order in cyberspace; Regulation over cyberspace; Ability-and-utility-oriented control (AUOC); Steps in data movement

Introduction

Information and communications technologies (ICTs) come from and have significant impact on the global society. Many human activities with functions and patterns different from that of traditional society have been facilitated by the globally connected computer networks. Previous ethical and legal discourses are undergoing serious challenge from newly emerged cyber-semantics. If we are going to set a limit between meanings of cyber- and traditional activities, there can be found some clearly defined, however controversial, characteristics. The conundrum happens when organisers of society have the same interests in guaranteeing the successful expansion of their immanent regulatory instruments from traditional society into cyberspace without a loss in enjoying their

existing power. Nothing would be tolerated in case it is simply an activity that takes place in cyberspace, other characters being the same as that in the meat space. We can perceive some particular cases as exceptions; however, they can only be seen as exceptions to the mainstream tendency. It could be well expected that online behaviours would have no more difference from their offline counterpart in respects of getting regulatory results.

For some time, cyberspace enjoyed some extent of contentment from evading regulation as stringent as on the traditional society. A variety of negative effects emerged and countries have growing eagerness to contain activities in cyberspace into their jurisdictions. Nevertheless, a string of impediments deferred the process of integrating online and offline “activities”. All countries are territorial-dependent, and no on single country has ever had claimed global control over all humans in the world, with rare exceptional situations where some countries extended their jurisdictions beyond their territories by domestic legal acts or according to international agreements. The networks-facilitated cyberspace has a virtually global reach in the sense of spatial concept, exactly going beyond single countries and in a certain sense incurring the ardour of countries to exercise control over it by one ultimate entity: a country, or an institution. However, it has never come true that a universal jurisdiction principle is accepted as a general rule in either meat space or cyberspace. Academia, legislature, and law enforcement agencies have all been devoted themselves to harmonising domestic laws or meliorating international laws in order that they are applicable to cyberspace in conformity with meat space.

Furthermore, cyber-activities have innovative players, processes, and objects. The new players are netizens hooked online through wire and wireless links, acting through transmitting digitalised information, and influencing status of objects without physical appearance in person. The identity of the players can effortlessly be concealed, the trace of their activities be eliminated, with their locality impossible to be spotted. Adding to these complexities are perplexities that even if they are identified they can still be involved in legal controversies, either that their activities regarded as legal by one country are denounced in another country, or vice versa.

We expect that the core arguments in this article concerning the approach to online content can also be useful in dealing with other online legal questions, such as unauthorised access to information systems, piracy of intellectual property, fraudulent schemes, destruction of data, defacement of websites, dissemination of malicious programmes and so forth. All these online activities with negative social evaluations have generalities in common, even though there are also many particularities. That is because of similar extent of social evaluations on these obnoxious activities that make countries to motivate their legal instruments to tackle them. Of these activities, online content has been one of the most controversial issues, over which many countries make efforts to exercise control. From the point of view of regulators, it is an urgent task to discover a route for installing previous rules in cyberspace regulation.

In determining the optimal selection from a variety of regulatory alternatives based on national orientation in cyberspace, we should first examine advantages and disadvantages of each option and reason which one has the highest meritoriousness capable of dealing with jurisdictional effectiveness and pecuniary efficiency.

Structure of the reasoning

Regulation of cyberspace has attracted great attention from academia since late 1990s. Many people have invoked laws of different countries for or against regulation of cyberspace. Therefore, there have been significantly different standpoints concerning whether cyberspace should be regulated, and if we give a positive answer, to what extent it should be regulated. In particular, online content may be the most controversial respects of such a disputation. In the U.S., for example, freedom of speech has been established on a firm constitutional foundation through its First Amendment. Oftentimes it has been interpreted in a broader way than many (if not any) of free speech provisions in the world. In China, for another example, both governmental and civil views, which usually distinguish between content considered legal or ethical and content considered illegal or unethical, are in favour of some kinds of regulation over online content (Fallows 2008). Even though people from the U.S. may assume that control of the Internet in China might be a discontented experience, majority of Chinese netizens seem not so resistant to such a way of control (*ibid.*). This fact indicates that different attitudes do not obstruct us from discussing ways of control.

This discussion is based on the assumption that some kind of regulation over cyberspace should be imposed, regardless of the extent to which such a regulation should be. Lessig's code approach (Lessig 1999) has (over)stated the role of code as a potential regulator (a subject, or a tool?). Kerr's perspectives approach (Kerr 2003) attempted to bridge the gap of understanding between cyberlegal problems and conflicts between internal and external perspectives. Weiser's competitive platforms approach (Weiser 2003) assigned each of cyber processes to a certain layer. Rather than calling them layers, I would simplify these aspects as nodes that comprising the whole chain of data movement. In practice, some others also mentioned different stages of data movement, such as Zittrain (2003), who divided the process into five stages: from source, to source ISP, to cloud, to destination ISP, and to destination. However, my typology would consider not only stages of data movement but also intervention of human elements with mechanical transmission and processing. In so doing, data movement will be considered as beginning with human intervention with mechanical transmission, without which no data can be input and no command can be sent for data processing and transmission. In this step, human intervention is a necessity for commencing the data movement through human-machine interaction. It is the human entity at the starting point of the run initiates the whole process, whatever the effect will take place. Subsequently, data movement will be realized in a step when human intervention is not a prerequisite but it can still be possible that human intervention is involved. This step is symbolised by machine-machine interaction, with or without human intervention. The third and last step ends with machine-human interaction that has impact on human entity at the destination. Here we use the term step instead of period, phase or stage by considering that the duration of the process of data movement is rather short, and that the beginning and the ending of the process are more like two temporal points than two periods. The only longer duration happens in between these two ends, that is, the movement itself, which is also rather rapid and instantaneous. People use such term as "synchronous," "synchronic," "synchronous," or "synchronized" to describe such a situation. Thus we establish a typology including three distinct steps in data movement: human-machine interaction step (HMIS), machine-machine interaction step (MMIS), and machine-human interaction step (MHIS).

Control at human-machine interaction step (HMIS)

Humans always predominate data movement. But humans also play different roles in data movement from the beginning users through deposition, hosting, transmission, and processing by machine to the end users. At human-machine interaction step of data movement, human acts more predominately than in other steps. It is these activities with predominate nature that primarily determine the human involvements at other steps, let alone mechanical involvements and human-machine interaction.

As far as online content is concerned, players at this step include online content authoring parties (OCAPs) and online service providing parties. OCAPs are those both individual and institutional users who write, create, demonstrate, perform, record, upload, review, publish, distribute, disseminate, propagate, lease, lend, sell by wholesaling or retailing, or have the content to enter the movement process by other means so that it can reach other users. Apparently, players at human-machine interaction step act more actively in putting data online. Besides authoring parties, online service providing parties are also involved in the initiation of this process by accommodating movement of content-related data.

Eliminating incentive of OCAPs may be the most effective option to exercise control over online content. If and only if potential authoring parties could no longer benefit, either financially or spiritually, from authoring, online content would no longer be authored. Thus the most effective control begins with control over authors. However, this effectiveness can not directly be translated into efficiency due to the geographical distribution of global users. Authorities are simply confronted with jurisdictional limits based on international political borders. Law enforcement is still operated in a rather conventional way that is reluctant to positively face jurisdictional conflicts, which is deepened by ideological, political, ethical, legal, procedural, methodological, and technical conflicts. As a result, to discourage authoring parties by various possible ways become an unfavourable idea.

Yet worse, once motivated authoring parties upload the content online, it is published to a media with a global audience and delivered on a nearly hybridly regulated platform. Even if the purpose of regulation is not for penalty itself, once spread, online publications can not simply be removed thoroughly. The existence and dissemination of such content become an eternal digital movement.

Now we have to turn to Internet service providing parties (ISPPs) who have certain ability to control data movement, even though their functions are originally not limited to do so. ISPPs may be immune from any liability in many situations, but they are imposed some kind of liability in some other situations. If we stop at discussing this issue only at the layer where ISPPs are supposed liable, it is a typical *mala prohibita* if ISPPs are imposed liability for their failure in fulfilling responsibilities that authorities would possibly assign to them. Because they are located in a condition where it is more possible to exercise control over online content authored by others, to assign them certain responsibilities, failing to fulfil which will be punished, is economically and judicially a more efficient way than attempting to prosecute authoring parties that are jurisdictionally impossible to prosecute.

ISPPs are usually more established, more organized and more centralized entities than authoring parties. They are more likely to act anonymously than single individuals and institutions. They are also likely to operate with more stable localities. These characteristics render ISPPs a status that the regulators can use to remove unfeasible content and even launch legal actions against ISPPs themselves.

ISPPs are not only passive in accepting authoritative commands, but they can actively exercise control over content within the scope of their services. For example, they have the capacity to take measures to direct content to where it is acceptable and avoid directing them to where it is unacceptable. In other words, ISPPs have much say on data movement: whether data move, when data move, where data move, or to whom data move. Thus, control over OCAPs can well be translated into control over ISPPs.

Control at machine-human interaction step (MHIS)

Online content consuming parties (OCCPs) are end users of data movement in the case of content-related transmission. They have both similarities with and differences from OCAPs in data movement. While OCAPs start up the process of data movement, OCCPs put the process of data movement to an end, ending in consuming: either downloading, reading, watching, listening, using, enjoying, borrowing, renting, redistributing, re-disseminating, or re-propagating, but mainly for their own consumption. Even though OCCPs as end users engage in passive acceptance and active mining of online content products (OCPs), their activities are passive in nature. If there is no online content existing for their consumption, these end users could never reach such OCPs in online content market (OCM). Thus it is a reasonable option for interest authorities to restrain their impulse to exercise control over activities of OCCPs. In particular, authorities of one country reluctantly have the motivation for impose certain liability on OCCPs in another country. Territorial jurisdiction stops before the borderline between countries.

It has never been a good idea to exercise jurisdiction on persons living in other political entities. The computer networks did not change the traditional concept much. Even if some people attempted to broaden the understanding of authoring activities to the extent that it covered the actual activities of reconstructing digits into complete files through downloading, viewing, browsing, retrieving and saving in magnetic media, they are increasingly put to an unfeasible place serving as the synonyms of “authoring” or “possession”. The applicability of rules against possessing or authoring such online content cannot be uncontroversially justified. Otherwise, to control individual and institutional OCCPs is confronted with the virtually same predicament as in the case of OCAPs: they are just similarly distributed in a geographically global space and control would be inefficient and ineffective. Morally or legal preventing such contents usually give place to technical measures, which are gradually invented to arm authorities all over the world to filter content that they separately classify as objectionable according to their own standards.

It happens that it is difficult for authorities to directly regulate each and every OCCP, and that there are also nodes directly serving end users. That is those nodes that have to take responsibility for controlling activities of OCCPs and those who fail to do so would be held liable for the

unfavourable consumptive activities involving retrieving of objectionable online content. Similar to ISPPs at the starting point of data movement, ISPPs at the end point of data movement also become the targets of authoritative regulation, for the sake of efficiency and effectiveness. ISPPs are neither end users nor regulators, but become controllers of end users and controlled by authorities. That's why ISPPs are usually not willing to orientate themselves as located in between end users and law enforcement.

Control at machine-machine interaction step (MMIS)

Control over activities of start users and that of end users in the chain of data movement with special regard to online content market proves problematic. Extended control over ISPPs that are adjacent to start and end users can partly be justified. Because there are altogether three steps in the process of data movement, we must now clarify the controllability of the interstitial step.

Quite a lot of players live on digitally linking start and end users. At this step, human elements are automatically played down by deep involvement of technological and technical solutions. Technologically, portals and search engines attract and facilitate users to harvest online content. There are technological means to provide some kinds of options for data movement. Obviously, machine-machine interaction is in practise dependent on regulatory direction from humans, who receive another level of regulatory direction from authorities.

The possibility of human intervention through technological and technical measures at the step of machine-machine interaction of data movement does not automatically mean that it is easy for portals and search engines to filter and prevent large quantity of moving data. In fact, imposing liability for omission to filter and prevent objectionable online content would be less efficient and effective than imposing liability for commission to providing hyper links. This is exactly where the responsibility and liability should be positioned. Creating an incentive for human interveners to bear a burden for doing something extra would not work better than creating an incentive for them not to do something unfavourable. To move somebody doing something extra beyond their duty while no compensation is provided, she/he would manifest some kind of inertness in reaction. In case of punishing somebody for doing something objectionable from the point of view of government, she/he would present a higher degree of coordination. Purpose of regulation is just located in coordination but not punishment. In designing a mechanism to subject human elements to coordinative data movement, OCM would be operated following its orbit of economic utility. In sum, human interveners at the machine-machine interaction step have certain degree of ability to exercise control over data movement by bearing additional of filtering and preventing data but have less utility to do so. On the contrary, they would have both ability and incentive to exercise control by not providing access opportunities for certain data.

Ability-and-utility-oriented control (AUOC)

Our analysis on regulation and control at different steps of data movement reveals that the official action must be within the ability of the controller so that it can be effective, and that it must be also out of utility of the controller so that it can be efficient. On the contrary of this conclusion is that

control by controllers without ability will be ineffective, while control by controllers without utility will be inefficient. Only control by controllers with both ability and utility will be effective and efficient. Based on this principle, only local authorities who fall in the same jurisdiction as where players who play negatively are located may actually exercise control over relevant step or steps of data movement. Those authorities without interest in affairs that players play negatively are monetarily discouraged from exercising control.

The logic in online content market is that, those who are able to exercise certain extent of control, who are assigned the responsibility for control and who fail to exercise due control would be held liable. These players seem to play in a broad “online” ground. However, when responsibilities are assigned to players, they do not simply mean to do something in favour of authorities. On the contrary, they sometimes simply mean not to do something unfavourable to the authorities or society. In other words, omission is not taken into account when liability is imposed, but commission renders the players into perfect liable status if such commission leads to data movement that disseminates objectionable content to OCCPs, who without such commission would not have access to such content, or who without such commission would have less numerous, frequent, or convenient access to such content.

However, ability is a must in considering to whom the responsibility should be assigned. To assign responsibility to players in a status unable to fulfil, would make it morally unjustifiable to hold them liable in law enforcement stage.

Control over online content market has to be exercised in a way balance ability and utility of concerned players. Ability only or utility only is a vacuous design of regulatory framework. Taking both of them into consideration would avoid dilemmas in justification, and efficiency and effectiveness.

Control over online content is neither designed to exclude as much users from the OCM, nor to prevent as much users from the beneficial consumption of content. Utility is a must in considering mechanism for control. To assign responsibility to players in a status unbeneficial, would make it economically inadvertent to move them fulfil their responsibility.

Conclusion

Because traditional spatial divide between jurisdictions has almost been precisely transplanted into cyber-laws, legal gaps of cyber-laws among different localities survived. This paper explored a control model, that is, ability-and-utility-oriented control, with special regards to regulation over Internet content, through an approach with emphasis on players in three different steps of data movement that are separately characterized by human-machine, machine-machine and machine-human interaction with different degrees of human intervention. According to this mode, the official action must be within the ability of the controller so that it can be effective, and that it must be also out of utility of the controller so that it can be efficient. Therefore, the nature of ability-oriented control and utility-oriented control can be and must be combined so that the best outcome can be expected.

Endnote

Ideas in this paper were developed over the years. An early version of this paper was published in a book entitled “*Social Order in Cyberspace*”, Amicus Law Books Division, ICFAI University, India, 2009. The book was printed in a small run and generally unavailable to external readers. This version of the paper, updated and revised, is to bring the ideas to a broader audience.

References

Fallows, D. (2008). *Few in China complain about Internet controls*. March 27. Retrieved December 2014, from <http://www.pewtrusts.org/en/research-and-analysis/reports/2008/03/27/few-in-china-complain-about-internet-controls>

Kerr, O.S. (2003). The problem of perspective in Internet law. *Georgetown Law Journal*, 91 (February), 357-405.

Lessig, L. (1999). *Code and other laws of cyberspace*. New York: Basic Books.

Weiser, P.J. (2003). The Internet, innovation, and intellectual property policy. *Columbia Law Review*, Vol. 103, pp. 534-613.

Zittrain, J. (2003). Internet points of control. *Boston College Law Review*, 44(2), 653-688.

Bibliographic information of this paper for citing:

Li, Xingan (2014). "Exploring into regulatory mode for social order in cyberspace." *Webology*, 11(2), Article 125. Available at: <http://www.webology.org/2014/v11n2/a125.pdf>

Copyright © 2014, Xingan Li.

LEGAL-SERVICE-ORIENTED ARCHITECTURE (LSOA) IN ELAWYER

Xingan Li*

Abstract

Legal services have long been practiced under a monopolistic mode, face-to-face consultation between lawyers and clients being the prototype. Pervasive use of information systems provides the possibility for clients to access legal services in a more cost-effective way. eLawyer is an electronic system assisting lawyers to provide and clients to receive legal services. In this paper, I would like to introduce current development in the respect of eLawyer. In this paper, a broad outlook on legal service is applied, and I will give some basic ideas about how the eLawyer should be structured and operated, which parties are involved, what kind of relationship they have, what services they transact, and what limitations there are in eLawyer services.

Keywords: eLawyer, information systems, legal services, Legal-Service-Oriented Architecture (LSOA)

Introduction

Legal services have long been practiced under a monopolistic mode, face-to-face consultation between lawyers and clients being the prototype. Pervasive use of information systems provides the possibility for clients to access legal services in a more cost-effective way. Lawyers have to consider role-transformation and service-transformation. The clients' requirement for change and the lawyers' willingness to transform provide eLawyer with a sturdy foundation.

The term "eLawyer" can be loosely defined as an electronic system more or less assisting lawyers to provide and clients to receive legal services. In this paper, I would like to introduce current development in the respect of eLawyer. As a website, eAvocat's self-introduction states that, "eLawyer is a management application for a law firm using Internet technology and that allows besides an easy management and monitoring of a law firm, easy access from clients to their dossiers and documents." (URL: http://www.amorphys.com/company/news/The_eLawyer_presentation_website_is_online_.html). In this sense, eLawyer has sense in overall eservices industry and deserves research. Friedman (1999, 2001a, 2001b) dealt with providing legal advice to clients through the WWW. However, legal advice is only a part of overall legal services. In this paper, a broad outlook on legal service is applied, and I will give some basic ideas about how the eLawyer should be structured and operated, which parties are involved, what kind of relationship they have, what services they transact, and what limitations there are in eLawyer services.

Parties involved and interaction process

Parties involved

Legal service is purely a knowledge work, whether people nominate it or not. It is a process that the client, who was not trained to have sufficient legal knowledge and skills, acquires legal advices from the lawyer, who was trained to have sufficient legal knowledge and skills, by paying a very big sum of commission. It is so that no state in the world provides sufficient resources in

* LLD, University of Turku, Finland (e-mail: xingan.li@yahoo.com).

training a great number of people to have sufficient legal knowledge to exercise law in the country. Only one in hundreds of thousands of people can be trained and granted a lawyer's qualification at the end of a long-lasting competitive procedure, and after she/he gets a license she/he can do so. Thus her/his knowledge and skills would be very expensive for potential clients to purchase and consume. Monopoly of resources in legal education lead to monopoly of knowledge and skills, and in turn leads to monopoly of market for legal services. One single lawyer cannot monopolize the market of legal services, yet the whole market is in fact monopolized by all the lawyers as a whole. This monopoly is usually supported by the state power. That's why this monopolistic status can be challenged by no one.

Unfortunately, unlike other services where people can create added-value by access to the existing market, transforming lawyer into eLawyer would not create more lawyers than before. eLawyer is operating in the old market and takes on a new outlook. It is not a force to change the monopolistic situation, but to simplify the process of human-human interaction which is a necessity in transaction of legal services. Similar transactions are prostitution, massage, medical operation, haircut, and so on. They are all examples of services that cannot be substituted by non-human-human interaction.

In this service, the two parties have different roles and status:

1. The service provider is lawyer (or in the name of attorney, solicitor, barrister, counselor-at-law, legal advisor, etc.). The transaction process of legal services can be simplified by adopting eLawyer. To search and hire a lawyer online save much of the client's offline attempt. Some kinds of or some parts of legal services can also be provided through eLawyer. Particularly, preparation for some kinds of legal forms can largely be submitted to the lawyer through eLawyer website, but the lawyer's personal involvement is still a must.

2. The service recipient may be plaintiff or pursuer, and defendant in civil and administrative cases; suspect or defendant in criminal cases; parties to the contract or agreement, and so on. All of these kinds of parties can be an individual, a group of individuals, or an organization, or a group of organizations.

Traditionally, relationship between the lawyer and the client is closely tied by human-human interaction. By eLawyer, the human-human interaction relationship between the lawyer and the client is only slightly intervened by the introduction of human-machine-human interaction.

Interaction process

In eLawyer services, a database of law might be grasped by the service provider. But access to the database is not necessarily a core service of eLawyer, because access to database itself could not constitute a part of legal advices. It can be said that law itself provides only general advices (proscriptions and prescriptions) to all citizens. But legal advices are those that targeted at detailed cases of the clients. Thus access to database of law does not constitute a core service of eLawyer, because a database is not a lawyer and no human-human interaction or even human-machine-human interaction is involved there. It can be seen as a human-machine interaction, a half interaction between human beings.

In practice, legal services are usually provided in particular situations, for example, in the court. When a lawsuit is heard in the court, at the moment, all parties must be present in person, or in special cases, at least the lawyer. So eLawyer has to go offline into the court, where the human-human interaction between the lawyer and the client is transformed into influential force over the human-human interaction between the client and the judge and the jury, so that the judge and the jury can have more knowledge about the situation of the client from a more professional point of view.

Beyond the introduction of the term stand-in-person, I reviewed and recognized that the previous thinking was limited to two extremes of legal services. One end is that legal services are

only provided as a kind of knowledge base for the clients through information system, without much effort of lawyers to assist them. A stand-in-person is not a must and never practically in charge of the service, once the legal database is ready for use. The other end is that legal services finally go to the field- mostly, a court. A stand-in-person become fully in charge of the entire service. Information systems are only assistance for building relationship between clients and lawyers.

Now, with the introduction of the term stand-in-person, I could further expand my discussion. That is, between the above extremes of legal services, there stand more forms of legal services that can be provided as composed of a proportion of automated computing and another proportion of stand-in-person intervention. Here, neither the automated computing nor the stand-in-person is completely responsible for the whole service. Rather than these two extreme forms, both automated computer and stand-in-person contribute to the establishment of relationship between clients and lawyers, to the maintenance of such a relationship, and to the fulfillment of the service object. During the process that lawyers collect commission and provide legal services to clients, clients pay commission to lawyers and accept legal services, information systems constitute a part of the human-human interaction.

Here is a case of eLawyer services provided as in a middle-of-the-way form. According to its self-introduction, LegalZoom.com was founded by attorneys who have worked at some of the most prestigious law firms in the US and have used their expertise to simplify the law and make it accessible for everyone. Many common legal matters, such as drafting a will, incorporating a business or filing a small claims action, are services that have a great market need, while most people do not want to spend the time, or the money to meet a lawyer. LegalZoom was designed to help clients quickly and affordably create estate planning documents, start a business, register a trademark and so on. From legal practice, preparation of legal documents and formalities is a service that is possible to be provided by lawyers with information systems to simplify the process, without the service quality being reduced.

As it is well known, traditional legal services have been solely a knowledge work. They could not be provided entirely without lawyers' personal intervention. In this sense, electronic legal services are at most substitute or supplementary to personal legal services. Thus in case there is any problematic situation, it is the only method for clients to seek help from stand-in-person, and for the lawyers to use their knowledge to resolve the problem.

The Self-service conception and eLawyer service

An ideal model of self-service may exclude any intervention of human elements from IT infrastructure. But other degrading models may involve less and less intervention of human efforts; at least, if there are any errors during the process of self-service, human intervention becomes necessary.

In order to give a broad understanding of the conception, we can look at a conspicuous example of Omenahotellit (Anckar and Patokorpi 2004). It is an idea that hotels are for the purposes of rest and sleeping, all other services, including entertainment, meeting and meal, being supplementary and thus being excluded from such hotels. Some supporting services, such as cleaning and security, are outsourced to specific companies. Beyond this, these hotels can be operated and managed by automated systems rather than any personnel. Exhibition of rooms, booking, payment, check-in and check-out are all realized through the Internet and terminals in the rooms. We can see a highly self-served model.

eLawyer, will not be as highly self-served as Omenahotellit. Legal services have a broad coverage and many different kinds of aspects, differing from consultancy that is highly dependent on knowledge of the lawyer to form-filling that is less dependent on knowledge of the lawyer (nonetheless the knowledge and intervention of the lawyer is still a must).

I think the difference comes from the processes and the results of different services. During the process of legal services, final decision-making is usually manipulated by official agencies but not lawyer or client. Thus the fulfillment of legal services does not mean that the client will realize her/his goal of buying the service. The lawyer has to do her/his best to use legal knowledge to assist the client to cater for the requirements of official agencies. Comparatively, in accommodation services there is not such a decision-making organ. Rather, accommodation services are decided solely by service provider and service consumer.

In addition, in the case of accommodation services, the results of some services have some extent of possibility of reversal and compensation. If there are some errors or faults, one party may give another party some kinds of pecuniary compensation and the other party may be satisfied by the money, additional services, or by finding services elsewhere. Legal services are different. If the clients failed in official decision-making because the lawyer did not provide qualified services, even if she/he gets compensation, she/he may not have an opportunity to get the same need met. Sometimes, the official decision may be final. Other times, the official decision may be appealed against and be reversed. But uncertainty of the final result is beyond the control of either the lawyer or the client.

Added value and compensation

Legal consultation is rather expensive all over the world. For example, in the US, hourly rates of attorneys are calculated by experience levels:

Experience	06-07
20+ years	425
11-19 years	375
8-10 years	305
4-7 years	245
1-3 years	205
Paralegals & Law Clerks	120

Source: United States Attorney's Office,
http://www.usdoj.gov/usao/dc/Divisions/Civil_Division/Laffey_Matrix_6.html

eLawyer service can reduce the attempt that the client searches, finds and hires a lawyer, and also reduce the attempt that the lawyer finds a client. The process of transaction in legal service can become simplified because of less transportation, communication, and face-to-face consultation. Most importantly, the expenses involved in face-to-face consultation are to be removed if no such consultation is involved, as in the case of LegalZoom.com.

The lawyer can collect compensation according to the complexity of the case, and the quantity and quality of the legal advices. For example, LegalZoom.com's incorporation service is priced according to three different kinds of packages:

The first is economy package, service of which is priced at \$139, covering basic incorporation preparation, such as preliminary clearance of your corporation's name, preparation and filing of Articles of Incorporation, customized corporate bylaws, including provisions protecting officers and directors from liability, and prepared resolutions of the first meeting of the Board of Directors.

The second is standard package, service of which is priced at \$239.00, covering basic incorporation preparation and some popular options, such as those included in the economy package, and Deluxe Corporate Kit embossed with your company name, official corporate seal,

twenty custom stock certificates with stock transfer ledger, Microsoft Accounting Express 2008, and medical expense plan forms.

The third is express gold package, service of which is priced at \$359.00, *being a all-inclusive rush package, such as those included in the standard package, and priority rush service (7-10 business days); over 40 essential business forms on CD-ROM, including employment and independent contractor agreements; Federal Tax ID (EIN) application preparation; S Corporation election preparation; and second day FedEx shipping of final package.*

It is said that the standard incorporation package was priced at about 1,480 US dollar by a lawyer. The primary cost of face-to-face consultation was saved because of provision of it as an eService.

Duration of the relationship

In eLawyer services, lawyer-client relationship can be diversified. In lawsuits, it is a kind of encounter relationship, that is to say, a short-term relationship. This kind of relationship expires when the procedure of the lawsuit is over. It is decided by a short-term demand and supply of legal services. For example, a suspect can only need a lawyer before his innocence is cleared or his conviction takes effect. Further interaction is only possible when relationship is established on new demand and new supply. But between the client and the counselor-in-law, it might be a long-term relationship. It is decided by a long-term demand and supply of legal services. For example, enterprises usually employ such long-term counselors-in-law.

eLawyer services are more valuable in encounter relationship. The client search, find and hire a lawyer only when she/he needs one (for example, <http://www.legalzoom.com>). Online availability of lawyers' profiles specialized in certain areas can be of special interest for the client in need. High-profile lawyers can have more competitive advantage over their low-profile counterparts in obtaining potential clients.

In long-term legal services, eLawyer service can also be valuable in reducing unnecessary face-to-face interactions between the client and the lawyer. This in turn creates a possibility to reduce counseling time and costs by taking advantage of counselor-in-law's familiarity of the enterprise's business and interests.

Roles of lawyer and client in service chain

The service chain involving the lawyer and the client is more complicated than any other service chains. There are special marketing procedures. In service chain, the following table can well illustrate the roles of the lawyer and the client:

Stage	Lawyer	Client
Marketing	Advertisements, free answers to questions, FAQ, Pricing standard, past experience (case study), partners and customers	Inquiring regarding basic information about the products and services provided
Negotiation	Describing capacity of the firm for relevant services	Describing service needed, providing necessary information about the service
Contract	Acting as a service provider	Acting as a service consumer
Performance and delivery	Preparing legal documents according to information provided by client, appearing in court or other judicial agencies with client, as an independent legal knowledge worker, but representing interest of the client	Submitting legal documents prepared by the lawyer to official organs, appearing in court or other judicial agencies with lawyer

Follow-up and evaluation	In general, the result is subject to official decision. The standard for whether the service provided is qualified is not based on whether the official decision supports the client's request. But if the client's goal is not reached, the client may claim the service unsatisfied by providing enough evidences.	In general, the result is subject to official decision. The standard for whether the service provided is qualified is not based on whether the official decision supports the client's request. But if the client's goal is not reached, the client may claim the service unsatisfied by providing enough evidences.
Invoice and payment	Holding the right to invoice	Having the liability to pay
Post-marketing	After client accepts the service, the contract fulfilled; if the client is unsatisfied, may refund.	Satisfied with services, the contract fulfilled; unsatisfied with services, requesting a refund for service fee but not official charges

Legal-Service-Oriented Architecture (LSOA)?

Now we are turning to the concept of SOA. I will not say much about how a LSOA looks like, rather, I think there is a critical factor influencing the basic orientation of a LSOA. Legal service has much specific elements absent in many other kinds of services. In considering designing or building a LSOA, these specific elements must be emphasized.

1. Legal service providers are mostly individual lawyers working in person. Even if they are legally organized, they deal with single cases with individuals' knowledge, skills, and experience. No substitute has yet been innovated in the world. The development of legal informatics did not liberate lawyers from physical work. Under such circumstances, the LSOA could not be built as an entirely automated system, which would simply not work.

2. Legal framework is the basis of legal services. However, legal framework, including laws and regulations, cases and decisions, is frequently changing with the development of many relevant factors in society. The LSOA shall have sufficient flexibility to adapt to new, fast and frequent changes in legal framework. Certainly, the central concern is for lawyers to learn new knowledge, skills and to have new experience.

3. Perception of facts in each individual case is a process of precise communication between clients and lawyers. Traditional face-to-face communication was and still is the most important means for clients to clarify facts to lawyers. Whenever lawyers have suspect about facts, clients shall provide detailed information. New ways of communication under LSOA must guarantee correct convey of information from clients to lawyers, or else it would lead to failure of the service.

4. Legal service requires particular trust and security. In all services, customers usually need to provide some information for maximizing their interests and benefits. Legal service is not an exception. But there are different concerns about privacy and security. For example, a criminal suspect might tell a lawyer all the details of his/her criminal act. The lawyer does not have the responsibility to provide a court with those details that are unfavorable for the criminal suspect, but to provide those favorable details. On the contrary, the lawyer has the obligation to keep those bad evidences secret. A successful LSOA must guarantee secured trust.

Limited possibilities

Unlike many other kinds of services, legal services are heavily based on human-human interaction, within which the lawyer provides legal advices to the client strictly according to

disputes and law. At least two parties, the lawyer and the client, are involved in the process. At least two kinds of knowledge, knowledge about the fact, and knowledge about law, form the basis of the interaction. Sometimes more parties are involved in the process and more respects of knowledge are necessary. Most importantly, the process of transmitting legal advices is usually undergoing a dynamic process, in which the client continuously supplements new situations that the lawyers must take into account, and in which some other parties continuously challenge the existing knowledge about fact stated by the client and the existing legal advice stated by the lawyer. Any other interaction cannot substitute the whole complex of human-human interaction, but, to a maximum extent, only part of it. From this point of view, we cannot expect that eLawyer completely exercises the functions of a lawyer.

Another factor that makes client-lawyer relationship special is that the lawyer is hired by the client. It means that the client only buys services from the lawyer within the scope of their contractual clauses. That the client buys is neither the personality of the lawyer, nor the whole knowledge and whole ability of the lawyer, nor something else physically perceivable. This relationship poses the lawyer as a special existence: on one hand, she/he stands with the client, independent of other parties; but on the other hand, she/he stands independent of the client, serving the client with her/his legal knowledge and skills. Thus the transaction of the legal service cannot be made through transfer a package and so on. In most cases, eLawyer might help to simplify the arrangement of human-human interaction by introducing a knowledge-based machine intermediary.

References

- Amorphys website, available at
http://www.amorphys.com/company/news/The_eLawyer_presentation_website_is_online.html
- Friedman, Ron (1999). Legal Web Advisors, available at
<http://www.prismlegal.com/index.php?option=content&task=view&id=49&Itemid=55>
- Friedman, Ron (2001a). The Business Case for Delivering Legal Advice over the Web, 2001,
<http://www.prismlegal.com/index.php?option=content&task=view&id=51&Itemid=55>
- Friedman, Ron (2001b). Should Litigators Use the Web to Deliver Legal Guidance to Clients? Available at
<http://www.prismlegal.com/index.php?option=content&task=view&id=48&Itemid=55>
- IBM (2008). Oracle and Progress/Sonic, SOA, available at
<http://moodle.utu.fi/mod/resource/view.php?id=23148>
- LegalZoom website, available at <http://www.legalzoom.com>
- Anckar, Bill, and Patokorpi, Erkki (2004). Omenahotellit: A Room with a View for the Internet Generation, Proceedings of the Tenth Americans Conference on Information Systems, New York, August 2004.
- Legal Service Shop, available at <http://www.freelawyer.co.uk/idx/index.asp>

Received for publication: 28.11.2014.

Review paper

UDK: 343.9

PHENOMENAL EXPLORATION INTO IMPACT OF ANONYMITY ON LAW AND ORDER IN CYBERSPACE

Xingan Li

Tallinn University Law School

SUMMARY

While information systems provide modern society with great convenience, it also poses new problems in maintaining social order. One of its negative influences is the anonymity of cyberspace, which makes identity tracing a noteworthy predicament which poses obstacles in detection and investigations. It has been found that cyber anonymity has critical impacts on criminal motivation, and the phenomena of victimization, and should be tackled on different layers including technology and law enforcement. The article explores how the anonymity symbolizes the cyberspace, what threats are posed by cyber anonymity against social order, what potentialities the anonymity has, how the trans-territorial anonymity was facilitated, and the real impact of anonymity on law and order in the information society.

Keywords: *cyber anonymity, dark figure, social order, law enforcement*

INTRODUCTION

The pervasion of information systems facilitates efficient access to information. While privacy is at high risk, anonymity, invisibility, and concealment of criminal traces become issues of broad concerns. The anonymity of cyberspace makes identity tracing a noteworthy predicament which poses obstacles in detection and investigations. This article deals with the formation and problem of anonymity in cyberspace in general, and

anonymity of cybercriminals in particular. It has been found that cyber anonymity has critical impacts on criminal motivation, and the phenomena of victimization, and should be tackled on different layers including technology and law enforcement.

Following this section, the article will explore how the anonymity symbolizes the cyberspace, what threats are posed by cyber anonymity against social order, how the anonymity protects cybercriminals, how the trans-territorial anonymity was facilitated, and the real impact of anonymity on law and order in the information society.

WRESTLING BETWEEN CYBER ANONYMITY AND LAW AND ORDER

Information systems have been increasingly critical in facilitating efficient access to information. Today, approximately 3 billion users, or 42% of the world population (Internet World Stats 2014) entered a new space networked by instant transfer of information. With much more information being accumulated, consumption of information becomes a double-edged process. While there is superfluous spam information, privacy is at high risk. Although people have appreciated the value and significance of cyber anonymity, negative concerns also emerge in anonymity, invisibility, and concealment of criminal traces. Cybercrime differs from traditional crimes in many different ways, including its universality and complexities, in particular, its anonymity, concealment, and invisibilities. The anonymity of cyberspace makes identity tracing a noteworthy predicament which poses obstacles in detection and investigations.

For example, in the case of spam, the e-mail can be both the instrument and the objective that are used in commercial, political, malicious, or illegal schemes. As a marketing and communications means, e-mail has been gradually abused. Unsolicited commercial mails (UCE) are typically sent anonymously or with a fabricated identity, and the recipients cannot discontinue successive messages. Messages of this kind furthermore consist of false or misleading headers, deceiving recipients to retrieve messages that they do not desire. Moreover, the recipients have no technique of expressing their inclination not to

receive such messages, and have no approach of requesting compensation even if they undergo loss. The abuse of e-mail has turned into a public annoyance in the online background. Even if the application of anti-spam services and technologies is escalating, the degree of spam is continuing to boost as swift (OECD 2004, pp. 2-3; OECD 2005, p. 6), becoming a predicament not only for individual e-mail accounts, but also for business accounts.

Another example is cyber terrorism. Despite the fact that cyber terrorism has not developed into a reality as lots of people worried at the end of 20th century, it becomes a gorgeous preference for modern-day terrorists for a number of reasons (Weimann 2004, p. 6). It is cheaper, more anonymous, aiming at a more massive target and number of targets, distantly conducted, and affecting a larger number of people globally. International society has barely implemented any countermeasures against conventional terrorism in the last few years. Weimann claimed that terrorism in cyberspace was more anonymous than conventional terrorist schemes. The fact that terrorists could exploit “screen names” or log on as a “guest user” makes it very difficult for security agencies and police forces to track down their real identity. What made it worse were that in cyberspace there were no physical barriers such as checkpoints to navigate, no borders to cross, and no customs agents to outsmart (*ibid.*, p. 6), making terrorists specially unidentified.

Maybe the most real threats and the most serious worries come from offences such as harassment and murder. In offences where information systems are used as means of committing verbal assault, threat, harassment, alarming, spam and fraud, the motivation of the perpetrator is to harass and to kill the victim. The function of the Internet as a means of communications and with a high anonymity of interaction often entraps the victims into unforeseeable dangers. In 2005, China Ministry of Public Security investigated 1,000 assassination cases, in many of which the criminals found the potential victims through the Internet (Yi 2006). In many criminal cases, stalkers and murderers find, follow, entice, and intimidate victims through the communication and interaction of various Internet services, usually anonymously.

On the other hand, concerning the legal status of cyber anonymity, people have long been disputing in vain. Conventional countermeasures and theories about crime

prevention were based on its material influence and on the material environment, although non-material factors have long existed, too. Activities in information systems can be expressed in a physically invisible form. What are physically visible in information systems are those physical existences, such as hosts and terminals, displayers, keyboards, mouse, and cables, while the mechanisms by which the computers function are invisible. Cyberspace is developed from information systems as an abstract space, differing from the material devices of information systems that include terminals and cables. It is invisible and intangible if compared with traditional space (Khosrow-Pour 1998, p. 440; Robertson 2000, p. 248; Dodge and Kitchin 2001, p. 81). When a web page is surfed, what can be seen is only the display of information on the screen. The web site is not physically a reading room where people can read magazines, newspapers and books, listen to audio records or watch videos, nor a marketplace, bank, street, or forum. It is merely a collection of web pages written in various mark-up languages, comprised of letters, numbers, and symbols in common use, but which facilitate the functions of linkage to other media, communicating with other people or directing to other services. The electronic address is not necessarily located along a street, in a building or even in a city, province, or country. In addition, the online services are usually provided in the manner of a remote transaction paid by means of digital cash or virtual money. Finally, the Internet users include individuals and institutions, but they do not necessarily appear in person or in an entity in a traditional library, forum, marketplace, bank, or along a street. It is entirely an invisible community in an invisible space—a group of anonymous netizens interact behind curtains or masks.

The invisibility of cyberspace worsens the situation caused by cyber anonymity, in the sense that criminals and offences in cyberspace become more concealed, while criminal justice faces greater difficulties.

ANONYMITY SYMBOLIZES CYBERSPACE

The disappearance of physicality in activities on the Internet symbolizes the new way for daily routines, and presents a chance for new practice and changes in faiths, positions, and manners (Zigrus 2001, p. 171). To a certain extent, Internet services are provided for

every user who owns a computer and a modem or cable linked to the server. The real identity of the user is not necessary for using the Internet. That is to say, a high degree of anonymity is achievable. Anonymity could indicate an intention to lie or not, to do something deceit or not. In the environment of online communications, particularly during interaction between remote strangers, information systems provide the possibility of maintaining anonymity, and we found that the users of information systems have the willingness to stay passively anonymous, not necessarily actively lying to their counterparts.

In the case of e-mail, it is uncomplicated to register an e-mail account with false information, or to send messages in the name of a certain person. These e-mails may not only infringe the legal rights and interests of the person of the counterfeited identity, but also are able to fabricate a rumour, slander other people, harm other people's reputation, or practise unfair competition to reduce the competitor's trustworthiness. No obligation of free e-mail service providers has been established to investigate the registrants' identity information. In addition, some web sites also provide anonymous e-mail services or sell anonymous e-mail software (Examples of such services and software can be searched out with search engines). Under such circumstances, the traceback of the real sender is impossible. Only where the providers' status is clear, under vicarious liability, can it be useful for law enforcement in some jurisdictions to hold the re-publisher responsible for the content of the original author (Edwards and Walde, eds. 1997, Part 4). E-mail has frequently been abused in an anonymous manner so as to realize a fraudulent scheme. This anonymity not only facilitates a lie, but may also support a fraud. In *R. v. Mastronardi* (2006 BCSC 1681), the accused, met the plaintiffs through an Internet dating service, during which the accused misrepresented himself as a single person and engaged in relationship with several victims. He represented himself as:

- (a) coming from a large, powerful and wealthy Sicilian family;
- (b) being a widower seeking a wife;
- (c) being a medical doctor with a specialty in gynaecology;
- (d) having hospital privileges and a clinic;
- (e) being a kind, caring and considerate person with positive family and moral beliefs, conveyed in conversations that went on for hours on end;

- (f) having elaborate and sometimes bizarre family and cultural traditions requiring highly submissive wives and amalgamation of finances to an account controlled by him;
- (g) as time went on, being third in command in mafia like family organization;
- (h) not wanting to date, but wanting to immediately enter into an intimate relationship, after which his culture and family regarded them as married;
- (i) once so married, his family required him to follow family and cultural traditions.” (paragraph 4)

In R. v. Farkas, the accused engaged in online fraud by using different e-mail addresses, mailing addresses, and user names, victimizing sellers and purchasers distributed in the U. S., Canada, and England (2006 ONCJ 121, 10 April 2006). In R. v. Reynolds & Ors, the accused engaged in online chat claiming himself to be a 16-year-old boy, attempting to make young girls expose their bodies and transmit photographs to him over the Internet ([2007] EWCA Crim 538 (08 March 2007)).

There are many ways by which people make efforts to detect lies, usually including various clues to emotion that may disclose the situation of lying (Ekman 1992, as cited in Howitt 2002, pp. 251-253). However, in the electronic lie, none of the clues can be useful, particularly those emotional ones, because there is no face-to-face interaction. Rather, the interaction itself is covered by a human-machine-human fig leaf.

Another field where people usually maintain anonymity is interaction in chat rooms. Accounting for a considerable fraction of the income of the commercial online providers, chat systems support synchronous communication, discussion on different topics, trans-territorial relationships on common interests, and ignorance of social status (Internet Crime Forum IRC subgroup 2001, pp. 7-9; Rowland 1998; Wilbur 1997, p. 5.). The biggest advantage of the interaction in chat rooms is that the user can keep anonymous at the beginning of the chat or remain anonymous during the whole process. Keeping anonymous means that people are able to fabricate identities that cannot be used to identify them. By disguising themselves, users can perpetrate fraud and many other related activities. This approach is definitely useful, too, in detection and investigation of crimes, where law enforcement uses falsified identity to allure and arrest suspects. For example, in United States v. Helder, (Eighth Circuit, No. 05-3387, 16 March 2006), an

undercover officer used a screen name and claimed to be a 14-year-old girl to entrap the perpetrator (pp. 2-4); in United States v. Baker (Seventh Circuit, No. 05-2499, 24 January 2006), an undercover officer used a screen name and claimed to be a 14-year-old boy to entrap the perpetrator (pp. 2-3); in United States v. Antelope (Ninth Circuit No. 03-30557, 8 June, 2004. Docket num. 03-30334, January 2005), the accused joined an Internet site advertising "Preteen Nude Sex Pics" and started corresponding with an undercover law-enforcement agent, in respect of whom the accused was entrapped when he ordered a child pornography video over the Internet; in United States v. McGraw (Tenth Circuit No. 02-1407, D. C. No. 01-CR-426-B, 2 December 2003), the accused was also caught by an undercover agent, with whom he expressed his interests in "having sexual contact with 'white males between the ages of 12 and 15,'" and arranged a encounter (See also R. v. Randall, Provincial Court of Nova Scotia 2006 NSPC 19, No. 1538177, 28 April 2006). The actual reality is that, in information systems, determining users' identity proves difficult, but not impossible.

POTENTIALITY OF ANONYMITY

Communicating anonymously is a great characteristic of the Internet environment. In using the Internet, anonymity can be kept from the beginning to the end. First, anonymous access to the Internet poses the most serious threat. In many countries, one of the most important forms of using the Internet is realized through cyber cafés or libraries, where anonymous users can access many of the online services. Definitely, there exist different situations in different countries. Compared with Finland where there are few cyber cafés in towns and cities, the cyber cafés in China have become the "third space" of school-aged juveniles besides home and school. The facilities and services in academic or public libraries are far less convenient for users than those in cyber cafés managed by private firms. An increasing number of hacking cases involving the Internet or Internet users are committed or conspired in cyber cafés.

Secondly, anonymous subscription to the Internet services raises the difficulty of identifying users. The personal information provided for the registration of an e-mail

account, the name and address of e-mail messages, and the authors' information in Usenet, etc., can all be fabricated. Keeping identity anonymous is favourable for the protection of users from victimization, but it also favours the hiding of perpetrators from being traced.

Thirdly, users can keep their identity anonymous in the process of online communications. There are also mechanisms for keeping complete anonymity by which one user can send messages to other users, and then the messages are transmitted to the final target, such as newsgroup, e-mail list, or a single e-mail account. What makes it more complex is that in the mechanisms the intermediary can only be a programme and may be in another jurisdiction (Kingdon 1994). This also reminds us that there exists the possibility of numerous transmitting points, by which messages are transmitted from one terminal to the next terminal, from that to the next in line, and so on, until the message reached the destination.

Tracing this transmitting process is theoretically possible. During the tracing process, the investigation is exactly the contrary to the process of transmission. Each time, the investigator can trace back one point.

It is likely that all points are identifiable. Nevertheless, as long as there is an unexpected element at any point, the tracing chain can be disrupted without reaching the original source. According to National Police Agency of Japan (1998), the possible examples include that the victim has no record of the Internet Protocol (IP) address; ISPs do not keep suitable records; hackers alter the logs; or some points are located in countries that have not criminalized hacking. As Koch (*Inter@ctive Week*, 10 July 2000) has pointed out, theories about detection remain theories, and they are too new to be tested in practice. Even if all the work of traceback is fulfilled, the actual value of this work may be discounted in a judicial process because of different locations and thus diversified jurisdictions.

Fourthly, the specific service or software can play further roles in hiding users. Cybercriminals usually establish anonymizers, which are systems particularly designed to invalidate technical identification of the source of communications (See Belgium's answer to the "Questionnaire 5: Have you received any reports from your law-enforcement authorities that have indicated an obstruction of their work due to the non-

existence of appropriate legal instruments concerning traffic data retention?” in Council of the European Union, Council doc. 11490/1/02 CRIMORG 67 TELECOM 4 REV 1, Brussels, 20 November 2002). In fact, this kind of service or software can also be conveniently obtained free of charge or at an inexpensive price from the Internet. Everyone who is online can get access to these tools and services. Such software is likely to be replicated and spread unlimitedly, creating a bigger population of hidden users who potentially threaten the security of information systems.

Although the anonymity of cybercriminals poses a series of questions, it is still the core of the “perfect environment” for the criminals. Levinson (2002, p. 455) said that anonymity is exploited by perpetrators of old crimes such as fraud, pornography, gambling, stalking and identity theft, or new crimes such as unauthorized access, denial of service, and malicious programmes. Yet it is at the same time welcomed by Internet users. People are constantly concerned that without online anonymity, it could be impossible to guarantee fundamental rights (COM(2000) 890 final, p. 20; National Police Agency of Japan 1998). It is not strange that the European Union Data Protection Working Party’s Recommendation recognized that online anonymity brings about a dilemma for governments and international organizations (The Article 29 Data Protection Working Party 2001): in particular, in maintaining human rights to privacy and freedom of expression, and combating cybercrimes (COM(2000) 890 final, p. 20). Philip (2002) warned that anonymity can provide users with “the courage to do the outrageous and sometimes even resort to illegal activities.”

Mitchell and Bunker (1997, pp. 707-711) have concluded that there are four characteristics in which cybercrimes are different from traditional crimes, that is to say, difficulties in detection, limited reporting, jurisdictional complexities, and resource constraint. All these four aspects fall under the broad characteristic of concealment. The concealment of cybercrimes has been brought about by other technological and human factors (Conly 1991; Clark 1996; Stephenson 2000; Mandia and Prosises 2003; Mohay and co-workers 2003; Vacca 2005; Johnson 2006).

Most of traditional offences are greatly observable due to apparent depredations, presence of witnesses, and so on. There are also traditional crimes that occur in private places and become less visible (Walsh 1983, p. 236). Unlike traditional threats where

criminals are physically present at the crime scene, cybercriminals are usually not present at the crime scene thus making apprehension difficult (Speer 2000, p. 260). In information systems, executing a command to delete files does not mean that the files are permanently deleted. What happens is merely that files are hidden due to a change in file names so that the files can be recovered. In *United States v. Angevine* (Tenth Circuit No. 01-6097, D. C. No. 00-CR-106-M, 22 February 2002), "the computer expert used special technology to retrieve the data that had remained latent in the computer's memory," though the accused had attempted to delete the relevant files. In *United States v. Upham* (First Circuit No. 98-1121, 12 February 1999), the investigator used the "undelete" function of a programme to recover deleted files from the deposit media, as primary evidence in conviction. In *Robertson v. Her Majesty's Advocate* ([2004] ScotHC 11 (17 February 2004)), the police recovered 347 deleted images from the unallocated space, and 878 images and 45 movies from deleted zip file within the disc. Only when a secure-eraser programme is in use, the files are permanently deleted. For example, in the case of *International Airport Centres, L. L. C., et al v. Jacob Citrin* (Seventh Circuit No. 05-1522, 24 October 2005) (p. 2). Skilful criminals can disable this kind of security mechanism, and conceal the data that might possible be taken as evidence in prosecution. Technological advances have both a positive impact on businesses and a negative impact on law enforcement (Institute for Security Technology Studies 2002). For example, in the DrinkOrDie case, the online software piracy group concealed its actions by various security measures: exchanging e-mails via private mail server using encryption; using a nickname to identify members, and communicating about group business only in closed, invite-only IRC channels; the FTP sites, where tens of thousands of pirated software, game, movie, and music titles were deposited, were secured by particular authentication mechanisms (U. S. Department of Justice, Press release, 17 May 2002). On the other hand, the available technological solutions have not completely met the requirement of data collection, log analysis, and Internet protocol tracing (American Society for Industrial Security 2004, p. 40). There is also the necessity for law-enforcement agencies to recruit personnel with "electrical engineering and computer-science backgrounds" (Fields 2004, p. B1);

Inevitably, critics point out that cyber police have extra incentives than combating

cybercrime, for example, asking for more money, more wiretap, bugs in computers and sell phones, weak encryption and permission to implement security technology, without more arrest following (Koch Inter@ctive Week, 10 July 2000).

Concealment of crimes has important economic effects. Stanley (1995, p. 2) stated that concealment of crime can decrease the incentives not to perpetrate, and increase the costs of law enforcement. Concealment of cybercrime demonstrates the low probability of punishment. In the U. S., only one in 100 cases was detected, one in 8 prosecuted, while only one in 33 prosecuted cybercrimes resulted in a prison sentence. That is to say, the likelihood that a cybercriminal would be put into prison was a one in 26,400 chance (Daler and co-workers 1989, p. 22), as compared with the likelihood of imprisonment in traditional bank robbery a one in three chance (*ibid.*). Law-enforcement agencies found that a majority of cybercrimes never reached the criminal-justice system. Even in the relatively few cases where a crime was reported, most often the criminal's identity was never discovered. As a consequence, as Radzinowicz and King (1977, p. 67) pointed out, "The calculation of chance is as applicable to the commission of crime as to many other activities." Given other factors constant, if cybercrime is more concealed than other offences, the potential perpetrators are more motivated to take illegal actions on the Internet, and thus more offenders of traditional crime will be prepared to migrate to cyberspace.

TRANS-TERRITORIAL ANONYMITY

Free flow of information from one state to another is a purpose of information systems (Directive 95/46/EC, Preamble (3); UN A/RES/51/162; Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Article 12), but trans-border flow is not free (The Convention mentioned above, Article 12 provides the limit on trans-border transfer of data). The trans-border information flux is accompanied by risks of crime of a similar nature. In any country, the court must have jurisdiction over the person or the subject-matter of a lawsuit. This works well with the current set-up of law-enforcement agencies that are territorial and are operating in different villages, towns, districts, cities, counties, states or provinces, or national

boundaries. Nevertheless, unauthorized access to information systems can be accomplished from virtually anywhere on the networks (See cases such as United States v. Tenebaum (Israel), 18 March, 1998, involving an Israeli hacking United States military computers; United States v. Gorshkov (W.D. Wash) 4 October 2002, Russian hacker; United States v. McKinnon I (E.D. Va.) and II (D. N.J.) 12 November 2002, British National Hacked into the U. S. Military Networks; United States v. Zezev (S.D. N.Y.) 1 July 2003, Hackers from Kazakhstan; United States v. Ivanov (D. Conn.) 25 July 2003, Russian hacker), because the communications capability of cyberspace allows criminals to conspire more easily, without geographical proximity to one another or to the target (Lenk 1997, pp. 126-135). The international characteristic of cybercrime is evident (National Police Agency 1998). In fact, some of the cases prosecuted have been of this nature, for instance, R. v. Kozun (2007 MBPC 7), where the forensic analysis of the computer of the accused disclosed that 165 separate users from 15 countries had traded through his computer. The computer was converted into an automated trading centre through a programme, by which 141 users had traded in the previous 13 days. The sphere of legal jurisdiction makes the cybercrime enforcement more complicated (Lee and co-workers 1999, p. 873). Smith, Grabosky, and Urbas (2004) concluded that the trans-national dimension of cybercrime posed four formidable challenges for prosecutors, who have to determine whether the conduct in question is criminal in their own jurisdiction, collect sufficient evidence to mobilize the law, identify the perpetrator, and determine his or her location, and decide whether to leave the matter to the local authorities or to extradite the offender (pp. 48-49).

Sinrod and Reilly (2000, p. 2) have pointed out that although some international organizations are examining cooperative mechanisms in the field of fighting against cybercrime, many of their members are slow in recognizing the urgency of the situation. The elimination of borders favours inter-jurisdictional mobility of crime. Due to the actual difficulty in establishing jurisdiction, even if a certain offence is detected, it is still uncertain whether the way can easily lead to punishment. In R. v. Burns ([2003] NICC 13(2) (12 September 2003)), where the accused cloned mobile phones, or exploited faults or loopholes in the internal phone systems of companies or organizations to make cheap or free calls at the expense of those companies or organizations, the court found

that:

“As the investigation progressed it became more wide-ranging and involved another suspect and its ramifications were such that it eventually spread to other parts of the United Kingdom, to Tokyo, to South America, as well as to New Jersey and Atlanta in the United States of America. Several large organizations in the United Kingdom, other police forces and international telephone companies were involved. When it became apparent to the police that they did not have either the specialist equipment or the necessary expertise to access much of the information, specialist firms had to be engaged. All of this took a great deal of time.” Reasonably, suggestions have been made to incorporate cyberspace into various jurisdictional frameworks. Nonetheless, this needs a great deal of time, agreement, and co-operation between countries, which are still struggling to take common actions.

Finally, it is worth noting that trans-national cases just make up a inconsequential part of cybercrime. No convinced conclusion can be drawn because it is probable that trans-national offences are not as prevalent as scholars have assumed. On the other hand, it is difficult to reveal these offences for reasons that scholars have laid bare. Or, it may be, that it is simply law enforcement does not put sufficient emphasis on these offences. Before credible data are available to give an answer to this question, we have certain reasons to claim that trans-national offences have sometimes of a dual nature: they do not appear as prevalent as domestic offences, but they are more difficult to detect and convict. In addition, because the investigation of trans-national offences is more expensive and time-consuming, law enforcement will not give more priorities to these offences than to cases that have happened “close to home”.

Because information systems alone are no longer subject to the physical limit of traditional countries, we can expect that many offences traditionally committed in neighborhoods, communities, and native areas now extend beyond national boundaries. Many other offences traditionally committed in a trans-border manner are becoming a means to acquire new markets in the more networked globe. Some new offences can, indeed, only be completed in a trans-national style. Trans-national crime can be seen as the counterpart of international trade in civil society, being an involuntary transaction

between perpetrators and the social order (in many cases, involving victims, but in many other cases, victimless).

For example, in *McKinnon v USA & Anor* ([2007] EWHC 762 (Admin) (03 April 2007)), the accused used his own computer in London and obtained unauthorized access to dozens of governmental computers of the U. S., from which he discovered the identities of certain administrative accounts and associated passwords. He installed remote control software on these administrative computers. The software enabled him to access and change data at any time.

Many people have taken it for granted that because computer networks are trans-national, naturally most crimes committed in relation to the networks are also trans-national. This poses a great concern among academia, law-enforcement agency, and legislature. However, this is still an unanswered question: firstly, information systems have crossed the national boundaries, but prosecuted offences are mostly confined within these boundaries; secondly, due to lack of an international arrangement of law and enforcement, few trans-national cybercrime offenders have been investigated; and thirdly, offences are mostly territory-dependent, and do not cross the border at all.

All these factors are responsible for the low likelihood of trans-national cybercrime, but, as we have seen and will see further, the absence of international legal harmonization and assistance mechanisms contributes primarily to the current invisibility of trans-national cybercrime.

IMPACT OF CYBER ANONYMITY ON CRIMINAL MOTIVATION AND VICTIMIZATION

Lack of punishment reduced the expected cost of the criminals, which were composed thus of moral costs and substantial costs, specifically, the perpetrators' necessary devices and labour in cybercrime. Because there was no cybercrime law, there was neither expected punishment nor the expected cost induced by the expected punishment. Under such circumstances, the probability of conviction equalled zero. The expected utility of the perpetrator almost equalled the utility of a situation in which crime went undetected or unpunished. According to an economic analysis of crime (Becker 1968, pp. 169-217),

those who are risk-indifferent are indifferent to detection and conviction. For those who are risk-lovers, cybercrime becomes a new cause, a new chance, a new challenge, and a new type of risk. For those who are risk avoiders, because of the low risk of detection and conviction rate of cybercrime, they transfer from other offences to cybercrime. Therefore, the number of cybercrimes and perpetrators will inevitably increase.

The low cost of cybercrime and the difficulty in detection and evidence collection create incentives for potential perpetrators. The nature of high intelligence, trans-territoriality, and high concealment of cyber transgress and cybercrime make it difficult to detect and investigate the cases (See Conly 1991; Clark 1996; Stephenson 2000; Mandia and Prosses 2003; Mohay and co-workers 2003; Vacca 2005; Johnson 2006). Starting from another standpoint, cybercrime surpasses the current capacity of public and private regulators to control (Grabosky 2000, p. 2). As for the transgressors or criminals, they usually only need to click the mouse or knock the keyboard at home or in the office in order to commit the illegality in a short time. The risks and costs are in cybercrime lower than those in traditional crime, while the benefits are higher. This cost-effectiveness further strengthens the mind of the perpetrator to commit cybercrime.

Cybercriminals have a greater advantage than most of the traditional criminals in respect of the low probability of arrest and conviction. Hatcher and co-workers (1997, pp. 397, 399.) have pointed out that many cybercrimes are not reported. The term “dark figure”, used by criminologists to refer to unreported or unrecorded crime, has been applied to denote undiscovered cybercrimes (UNCJIN 1999, Paragraph 30). As Radzinowicz and King (1977) pointed out that, “The recorded figures of crime are huge but the reality behind them everywhere looms far larger. The sinister word dunkelziffer (dark figure) was coined at the turn of the century to express this hidden reality.” (p. 42). Many intrusions are not detected for a variety of reasons (COM (2000) 890 final, p. 11). Cybercrimes can well be described as hidden crimes, which is used by Cook (1997) to denote under-reported or under-recorded crimes such as domestic violence, sexual assault, and racial harassment (p. 55-58), the counterpart of which is “hidden victims,” denoting the victims of the “hidden crimes” (p. 127).

At the same time, victims of cybercrime are keen to be hidden victims (Cook 1997, p. 127). The usual “motives for silence” pertaining to victimization may fall into one of the

following categories: 1. The idea that the victimization is not worth the mobilization of justice; 2. Involvement; 3. Pressures of fear; 4. The perturbed accessibility of police and court; and 5. The ignorance of events by the police (Radzinowicz and King 1977, pp. 38-40).

In sketching the victim decision-making, Greenberg and Ruback (1985) have established a three-stage model: the victim judges whether the event is a crime, evaluates its seriousness and decides what to do (Greenberg and Ruback 1985, as cited by Feldman 1993, p. 26). Before these stages, one stage that is more essential should be included, that is, whether the victim knows the event. If this is the case, the reporting of cybercrime might stay at a lower level, because cybercrime is imperceptible and thorny to notice; it is much trickier for the victim to judge whether the event is a crime and to estimate the losses; and the victim has less awareness of whether there is an agency to report the crime. The limited reporting of the cybercrime has been noted more than 20 years ago by Parker and Nycum (1984, p. 313), who studied the invisibility of computer crime. At present, the Internet's virtual environment has made the circumstances still poorer. Auspicious progress in proving material evidences in traditional crimes was made in late 1980s when DNA tests were first introduced (Levinson 2002, p. 537). Nonetheless, digital evidence in computer crime is untouched by such high-technological testing measures. The invisibility of cybercrimes is based on numerous factors, either technical or artificial (UNCJIN 1999, Paragraphs 30, 31). Sometimes, the straightforward cause is that the victims are not enthusiastic to report, or even do not know where to report the case (Salgado 2001). The acknowledged reasons for the reluctance to launch legal actions are principally fear of undesirable publicity, public humiliation or loss of goodwill, loss of investor or public confidence, resulting economic consequences such as the panic effect that this information would create on their stock prices (See Carter 1995, p. 21; Roush 1995, pp. 32, 34; Gelbstein and Kamal 2002, p. 2; McKenna 2003), and exposure to future attacks (COM (2000) 890 final, p. 11). The UN suggested that these factors have a momentous impact on the detection of cybercrime (UNCJIN 1999, Paragraph 31).

Yet there are other reasons for the victim to remain silence. While many people are vigorous in maintaining their interests and rights, some people view victimization as

their own malfunction in life and profession and are not enthusiastic to expose the reality of their failure to any individuals and institutions, so as not to make public their own disadvantage.

Therefore, it is unavoidable that the rate of unidentified instances of cybercrimes has increased as a consequence. The 2013 Australian Cyber Crime and Security Survey Report summarized the reasons why respondents did not report cyber security incidents, 44% of them said “there are no benefits of reporting”; 44% chose “other”, meaning that the incidents and the consequences were minor, and that the incidents were reported internally and managed by corporate policy; 20% said that “the attackers probably wouldn’t get caught &/or prosecuted”; 16% of them “did not know”; and 12% worried about “negative publicity for the organisation” (CERT Australia 2014, p. 35). This and other similar surveys has indicated the percentages of respondents identifying each stated rationale as being very imperative in their assessment not to report computer intrusion. At the same time, it is worth noting that the reasons are subject to changes in each yearly study.

CONCLUSION

Without ignoring all its merits, cyber anonymity has deep impact on occurrence of cybercrime, mostly reducing the potential likelihood of detection and thus its costs. In fact, anonymity may to some extent encourage potential perpetrators to take the risk. On the other hand, victims may lose opportunities to make judgment on whether or not it is of their interest to interact with hidden perpetrators. Once crime occurs, anonymity further hinders law enforcement from detecting and investigating.

In recent year, wrestling between claims for and against cyber anonymity has been continuing. However, there has some new advancement in judicial sector. The European Union Court of Justice issued a decision on May 13 2014, in case C-131/12 (Google Spain SL, Google Inc. v. Agencia Espanola de Proteccion de Datos, Mario Costeja Gonzalez), ruling that the “right to be forgotten” is embedded in the provisions of Directive 95/46/EEC (Iglezakis 2014, p. 4). The right to be forgotten is a special field of cyber anonymity. If cyber anonymity is not imposed any limit, vulnerable users and

incompetent law enforcement cannot cope with problems accompanying it. Therefore, the right to be forgotten applies only where the information is “inaccurate, inadequate, irrelevant or excessive for the purposes of the data processing” (para 93 of the ruling). the Court unambiguously spelt out that the right to be forgotten is not unconditional but will always have to be “balanced against other fundamental rights”, for instance the freedom of expression and of the media (para 85 of the ruling). Absolute freedom of anonymity should not be allowed as the case in the real society. There is a necessity to balance the needs to protect privacy and prevent cybercrime (Shinder, 2011).

REFERENCES

1. American Society for Industrial Security (ASIS). 2004. Cybercrime-Fighting Tools Still Lacking, *Security Management*, no. 40.
2. Becker, G. S. 1968. Crime and Punishment: An Economic Approach, *Journal of Political Economy*, vol. 76, pp. 169-217.
3. Carter, D. L. 1995. Computer Crime Categories, *Law Enforcement Bulletin*, U. S. Department of Justice: Federal Bureau of Investigation, vol. 64, no. 7, pp. 21-26.
4. CERT Australia. 2014. The 2013 Australia Cyber Crime and Security Survey Report. Commonwealth of Australia.
5. Clark, F. and Dilberto, K. 1996. *Investigating Computer Crime*, Boca Raton, Florida: CRC Press LLC, 1996.
6. Commission of the European Communities. 2000. *Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-Related Crime*, COM (2000) 890 final.
7. Conly, C. H. 1991. *Organizing for Computer Crime Investigation and Prosecution*, Darby, PA: Diane Publishing.
8. Cook, Dee. 1997. *Poverty, Crime and Punishment*, London: CPAG.
9. Daler, T., Gulbrandsen, R., Melgrd, B. and Sjølstad, T. 1989. *Security of Information and Data*, Chichester: Ellis Horwood.
10. Debose, B. 2004. Kerry Says Threat of Terrorism Is Exaggerated, *The Washington Times*, 29 January.

11. Dodge, M. and Kitchin, R. 2001. *Mapping Cyberspace*, New York, New York: Routledge.
12. Edwards, L. and Walde, C. (eds.). 1997. *Law and the Internet - Regulating Cyberspace*, Oxford: Hart Publishing.
13. Ekman, P. 1992. *Telling Lies: Clues to Deceit in the Marketplace, Politics, and Marriage*, New York: Norton.
14. European Commission. 2014. Factsheet on the right to be forgotten ruling C - 131/12. Retrieved 5 Feb. 2015, from http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf
15. Fields, G. 2004. Cyberexperts and Engineers Wanted by FBI, *Wall Street Journal*, B1, 6 April.
16. Gelbstein, E., and Kamal, A. 2002. *Information Insecurity: A Survival Guide to the Uncharted Territories of Cyber-threats and Cyber-security*, the United Nations Information and Communications Technology Task Force and the United Nations Institute for Training and Research.
17. Grabosky, P. 2000. Cyber Crime and Information Warfare, in Proceedings of the Transnational Crime Conference, Canberra, 9-10 March. Retrieved 5 Feb. 2015, from <http://www.aic.gov.au/conferences/transnational/grabosky.pdf>
18. Greenberg, M. S. and Ruback, R. B. 1985. A Model of Crime Victim Decision Making, *Victimology: An International Journal*, vol. 10, pp. 600-616.
19. Hatcher, M. and co-workers. 1999. Computer Crimes, *American Criminal Law Review*, vol. 36.
20. Howitt, D. 2002. *Forensic and Criminal Psychology*, Essex, England: Pearson.
21. Hunt, Allan. 1993. *Explorations in Law and Society: Towards a Constitutive Theory of Law*. New York, London: Routledge.
22. Iglezakis, I. 2014. The Right to Be Forgotten in the Google Spain Case (Case C-131/12): A Clear Victory for Data Protection or an Obstacle for the Internet? Retrieved 5 Feb. 2015, from <http://dx.doi.org/10.2139/ssrn.2472323>
23. Institute for Security Technology Studies (ISTS). 2002. *Law Enforcement Tools and Technologies for Investigating Cyber Attacks: A National Needs Assessment*.

24. Internet Crime Forum IRC Subgroup. 2001. *Chat Wise, Street Wise-Children and Internet Chat Services*.
25. Internet World Stats. 2014. World Internet Usage and Population Statistics – June 30, 2014 Mid-Year Update. Retrieved 5 Feb. 2015, from <http://www.internetworkworldstats.com/stats.htm>
26. Johnson, T. A. 2006. *Forensic Computer Crime Investigation*, Boca Raton, Florida: Taylor and Francis Group.
27. Khosrow-Pour, M. 1998. *Effective Utilization and Management of Emerging Information Technologies*, Hershey: Idea Group Publishing.
28. Kingdon, J. 1994. Shooting the Messenger: The Liability of Internet Service Providers for Prohibited Expression. Retrieved 5 Feb. 2015, from <http://www.catalaw.com/logic/docs/jk-isps.htm>
29. Koch, L. Z. 2000. Open Sources Preventing Cybercrime, *Interactive Week*.
30. Lee, M. and co-workers. 1999. Electronic Commerce, Hackers, and the Search for Legitimacy: A Regulatory Proposal, *Berkeley Technological Law Journal*, vol. 14, no. 2, pp. 839-885.
31. Lenk, K. 1997. *The Challenge of Cyberspatial Forms of Human Interaction to Territorial Governance and Policing, The Governance of Cyberspace*, New York: Routledge, pp. 126-135.
32. Levinson, D. (ed.). 2002. *Encyclopaedia of Crime and Punishment*, Newbury Park, CA: Sage Publications.
33. Li, X. 2008. *Cybercrime and Deterrence: Networking Legal Systems in the Networked Information Society*, Turku: Uniprint.
34. Mandia, K. and Prosise, C. 2003. *Incident Response and Computer Forensics*, Emeryville, California: McGraw-Hill/Osborne.
35. McKenna, B. 2003. United Kingdom Police Promise Charter to Guard Good Names, *Computers and Security*, vol. 22, no. 1, pp. 38-40.
36. Mitchell, S. D., and Bunker, E. A. 1998. Private Intrusion Response, *Harvard Journal of Law and Technology*, vol. 11, no. 3, pp. 699-732.
37. Mohay, G., Byron, C., Vel, O., McKemmish R., and Anderson, A. 2003. *Computer and Intrusion Forensics*, Norwood, Massachusetts: Artech House.

38. NPA. 1998. *The Situation of High-tech Crime and the Suppression of Police, Japan Police White Paper*, Tokyo: National Police Agency.
39. O'Brien, T. 2004. Risk and Conflict Challenges for New Zealand, *Auckland War Memorial Museum Symposium Push for Peace*.
40. OECD. 2004. *Second Organization for Economic Cooperation and Development Workshop on Spam: Report of the Workshop*, JT00174847, Busan, Korea.
41. OECD. 2005. Task Force on Spam, Spam Issues in Developing Countries, DSTI/CP/ICCP/SPAM(2005)6/FINAL, Paris, France.
42. Parker, D. B., and Nycum, S. H. 1984. Computer Crime, *Communication of the ACM*, vol. 27, no. 4, pp. 313-315.
43. Philip, A. R. *The Legal System and Ethics in Information Security*, SANS Institute, 2002. Retrieved 5 Feb. 2015, from <http://www.securitydocs.com/go/1604>
44. Radzinowicz, L. and King, J. 1977. *The Growth of Crime: The International Experience*, London: Hamish Hamilton.
45. Robertson, S. 2000. The Digital City's Public Library: Support for Community Building and Knowledge Sharing, in Toru Ishida and Katherine Isbister (eds.) *Digital Cities: technologies, Experiences, and Future Perspectives*, Springer, pp. 246-260.
46. Roush, W. 1995. Hackers: Taking a Bite Out of Computer Crime, *Technology Review*.
47. Rowland, D. 1998. Cyberspace - A Contemporary Utopia? *The Journal of Information, Law and Technology*, vol. 1998, no. 3. Retrieved 5 Feb. 2015, from http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/1998_3/rowland/
48. Salgado, R. P. 2001. Working with Victims of Computer Network Hacks, *USA Bulletin*, vol. 49, no. 2.
49. Shinder, D. 2011. Online Anonymity: Balancing the Needs to Protect Privacy and Prevent Cybercrime. Retrieved 5 Feb. 2015, from <http://www.techrepublic.com/blog/it-security/online-anonymity-balancing-the-needs-to-protect-privacy-and-prevent-cybercrime/>

50. Sinrod, E. J., and Reilly, W. P. 2000. Cyber-Crimes: A Practical Approach to the Application of Federal Computer Crime Laws, *Computer and High Technology Law Journal*, vol. 16, pp. 177-232.
51. Smith, R. G., Grabosky, P. and Urbas, G. 2004. *Cyber Criminals on Trial*, Cambridge: The Press Syndicate of the University of Cambridge.
52. Speer, D. L. 2000. Redefining Borders: The Challenges of Cybercrime, *Crime, Law and Social Change*, vol. 34, pp. 259-273.
53. Stanley, T. J. 1995. Optimal Penalties for Concealment of Crime, *Economics Working Paper Archive*.
54. Stephenson, P. 2000. *Investigating Computer-Related Crime*, Boca Raton: Florida: CRC Press LLC.
55. The Article 29 Data Protection Working Party. 2001. Fourth Annual Report on the Situation Regarding the Protection of Individuals with Regard to the Processing of Personal Data and Privacy in the Community and in the Third Countries Covering the Year 1999.
56. UNJCIN. 1999. International Review of Criminal Policy -United Nations Manual on the Prevention and Control of Computer-Related Crime, *International Review of Criminal Policy*, nos. 43 and 44.
57. Vacca, J. R. 2005. *Computer Forensic: Computer Crime Scene Investigation*, Hingham, Massachusetts: Charles River Media.
58. Walsh, D. P. 1983. Visibility, in Dermot Walsh and Adrian Poole (eds), *A Dictionary of Criminology*, London, Boston, Melbourne and Henley: Routledge and Kegan Paul.
59. Weimann, G. 2004. Cyberterrorism: How Real is the Threat? *United States Institute of Peace Special Report*, no. 119.
60. Wilbur. S. 1997. An Archaeology of Cyberspace: Virtuality, Community, Identity, in D. Porter, (ed.), *Internet Culture*, London: Routledge, pp. 5-22.
61. Yi, M. 2006. Associated with Traditional Crime, Cybercrime Threats Citizens Safety, *Huanghai Morning Newspaper*, 27 January.
62. Zigrus, I. 2001. Our Virtual World: The Transformation of Work, Play, and Life via Technology, IGI Global.

CYBERSECURITY AS A RELATIVE CONCEPT

Xingan LI

Abstract: Based on the relativity of the concept of cybersecurity, this article analyzes the economic impact of cybersecurity breaches, identifies cybersecurity as a private good that should be provided mainly by the private sector. However, public provision is also necessary when severe security breaches occur and liability mechanisms should be triggered.

Keywords: Cybersecurity, Illegal Behavior, Economic Analysis.

Introduction

The Internet has become a critical infrastructure for both public and private sectors and has brought new levels of productivity, convenience, and efficiency. The increasing incidents of Internet attacks representing examples of how vulnerable the information systems are, how far the offensive technology outpaces the defensive technology, how easy various malicious programs are created and how smart they can spread all over the Internet rapidly, have started to impact the practical facets of our lives. At the same time, the attackers are able to conceal their attacks by disabling logging facilities or modifying event logs, so their activity goes undetected. Even worse, some automated programs have been designed to specifically disable anti-virus software or penetrate firewalls. The security violations have multi-dimensional impacts on both consumers and businesses, including time, human resources, monetary losses and psychological losses.

The Internet and the larger information infrastructure are not secure.¹ McCormick identified five reasons why Internet is vulnerable: failing to enforce policies, ignoring new vulnerabilities, relying too much on technology, failing to thoroughly investigate job candidates, and expecting too much from technical skills.² These risks cause serious insecurity problems in the information society.³

While the governments have made efforts to better secure their own computer networks to prevent terrorists from hacking into computer systems, the governments have been increasingly concerned that the private sector is vulnerable to cyberterror-

ism. The question being asked is whether private businesses provide enough cybersecurity, or some form of government involvement is justified. Many empirical studies examined the economic impact of cybersecurity breaches. Theories diversify in regarding the cybersecurity as an externality,⁴ a public good,⁵ or a private good.⁶

Based on the concept of relative cybersecurity, this paper analyzes the economic impact of cybersecurity breaches, whether cybersecurity is a public good or a private good. It also establishes liability mechanism for cybersecurity breaches.

Impact of Cybersecurity Breaches

Increasing Investment of Users in Cybersecurity

The users' investment in cybersecurity takes on the tendency of increasing. Although exact statistics on these expenditures is unavailable, the add-up of global users' financial costs will reach a surprising figure. According to a survey conducted by the Computer Security Institute (CSI) and the Federal Bureau of Investigation (FBI), nearly all of the companies surveyed in 2005 used anti-virus software, firewall, and some measures of access control. Besides the hardware and software, the organizational users also have to employ security personnel or institutions to maintain their systems. These measures induce the increase of the investment of network users. But in fact, security measures can hardly ever be a perfect assurance against damage and accidents. Absolute security becomes too expensive to be reasonable.⁷

Frequent Occurrence of Cybersecurity Breaches

Although the investment in cybersecurity is increasing year by year, the breaches still occur frequently. The potential for information security breaches, as well as the magnitude of potential losses associated with such breaches, has been confirmed by empirical studies.

The annual surveys on information security breaches have pointed out that cybersecurity breaches are ubiquitous. The 2005 survey conducted by CSI and FBI revealed that 56 percent of the surveyed 693 U.S. computer security practitioners acknowledged unauthorized use of a computer in their organization in the last 12 months.⁸ CERT Coordination Center reported that the computer security vulnerabilities increased nearly 35-fold during one decade with 171 separate holes reported in 1995 and 5,990 reported in 2005.⁹ In the recent years, the publicly disclosed virus attacks are hitting the global computer users in an accelerated speed, even though many of the users are unaware of, or unwilling to report the losses.

Increasing Costs of Cybersecurity Breaches

As a consequence of the frequent occurrence of cybersecurity breaches, the losses of these breaches are increasing as well. The losses can be divided into direct and indirect, tangible and intangible, and short-term and long-term. Neumann stated that costs of cybercrime are difficult to measure; however, these costs are reasonably substantial and growing rapidly.¹⁰ Scholars proposed various models to try to measure the costs of security breaches, such as in the Forrester Research. Howe and colleagues' analysis indicated that, if the perpetrators were to unlawfully transfer \$1 million from an online bank, the financial influence to the bank would reach \$106 million.¹¹

The direct losses are those directly involved in the attacks, including interruption of business, destruction of software and hardware, expenditure on recovering the systems, installation and update of security means, recruiting security personnel, etc. The indirect losses are losses indirectly related to the attacks, such as reduction of consumers, decrease of stock prices, etc. The other kinds of losses are also easy to emerge.

The 2005 CSI/FBI survey noted that, of the 639 respondents that were willing and/or able to estimate losses due to security breaches, such breaches resulted in losses close to \$130 million.¹² On the other hand, Lukasik claims that cybercrime costs are essentially doubling each year.¹³ The problem becomes even more complex when one considers the "black figure" of these crimes. Ullman and Ferrera mentioned that, according to FBI estimates, only 17 percent of computer crimes are reported to government authorities.¹⁴

Relativity of the Cybersecurity Concept

There are various answers to the question "What is cybersecurity?" Cybersecurity is a comparative concept. On one hand, it includes the comparison between security and attack techniques. On the other hand, it includes comparison between different security techniques and measures. Considering the comparison between the techniques for security and attack, it is publicly well recognized that the attack techniques develop faster than the security techniques, regardless of the reasons. In other words, the hardware, the software, or the other information system components are always vulnerable and this fact can be exploited. We could call this the absolute level of security. Considering the comparison between the different security techniques, the existence of different environments, the possession of different hardware, software and other equipment, and the adoption of different security techniques, all this leads to difference in the level of security. Therefore, each of the individual or organizational users has a different security level.

Some viewpoints regard cybersecurity as an externality.¹⁵ Camp and Wolfram point out that if a company does a poor job at cybersecurity, other companies may be affected negatively. Thus, the cost is an externality to the owner of the infected machine.¹⁶ However, if we identify cybersecurity as an externality, it is inevitable that to the extent investments in computer security create positive externalities, too little will be provided.

Security is not the reason that drives the attackers to violate security and launch attacks, nor the condition that facilitates the attacks, but the target that the attacks aim at. In fact, there is no clear boundary between security and insecurity. Security and insecurity have only quantitative difference, but no quality distinction. Neither absolute security nor complete insecurity exists. That is to say, security and insecurity should be considered as security between zero percent and 100 percent. Therefore, security is a relative concept. The security of a higher level is security, while the security of a lower level is insecurity.

Although the information systems on the Internet all have a similar framework, they lack any central control system and are uncontrollable. Not only the physical system, but also the operational process is uncontrollable. Thus, to a great extent, the security of the Internet depends on the security measures taken by the end users, either individuals or organizations. However, the security measures of individual and organizational users are widely different due to the difference in hardware, software, and human resources.

The level of security of the end users on the network is different; an absolute value of security does not exist. Security is just a comparison of relative values. It is both the result of comparison between users and the comparison between past and present, i.e., horizontal and vertical comparison. Due to the large number of network users and the rapid change in the network environment, the result of this comparison changes constantly. In general, a higher level security will change quickly into a lower level security (insecurity) with transformation of techniques and the environment. Therefore, the cybersecurity measures have to be updated and renewed timely, frequently, and efficiently.

If the cybersecurity measures cannot be updated and renewed in a timely, frequent and efficient manner, vulnerabilities might occur. Vulnerability is not the security or insecurity themselves, but a factor that makes it impossible to realize perfect security, and an extra loophole caused by the external factors in the investor's production of the expected complete security. It is the natural adversary of the security product, i.e., flaws that can be detected and exploited by the potential attackers to commit harm and cause loss.

Table 1: Classical Division of Goods in Economy.¹⁷

Classic Division of Goods in Economy	Exclusion from Consumption	
	YES	NO
Competition in Consumption	YES	Private Good: Food, Clothing, Toys, Furniture, Cars...
	NO	Club Good: Private Schools, Cinemas, Clubs...
		Common Good: Natural Environment
		Public Good: National Security (Army and Police Forces)

Provision of Cybersecurity as a Private Good

In economics, goods are traditionally classified into four categories as listed in Table 1.

Besides other issues, private good and public good can be generally regarded as a pair of opposites. The main features of the private good are excludability and rivalry. According to Samuelson,¹⁸ public good is a good that produces a positive externality and which is characterized by non-rival consumption and non-excludability. The private provision of private goods, or public provision of public goods are not the unique ways in providing these two kinds of goods (let us not consider the other kinds of goods here). The ways of provision of these two kinds of goods can be illustrated as shown in Table 2.

The public good is usually confronted with the problem of being underprovided or not being provided when it is put on the private market. Such a problem appears in providing cybersecurity. Generally, a higher level of cybersecurity would benefit both the individual or organizational owner and users other than the owner. Because insecure computers are vulnerable to be manipulated to launch attacks against other computers, it is reasonable to assume that if an owner maintains a higher level of cybersecurity, the other users' computers may experience a lesser risk of being attacked. Then the other users would have the good reason to reduce their investment in security protection. The computer users' security provision only diminishes the probability of the others' computers being attacked. However, since individuals are not generally liable for the damage caused when a hacker uses their computer, they do not benefit from the increased security.¹⁹ And because users with ability to provide security do not benefit, they will fail to provide it. The same applies to other computer

Table 2: Ways of Provision of Private Goods and Public Goods.

<i>Different Ways of Provision of Different Goods</i>	<i>Private Provision</i>	<i>Government Provision</i>	<i>Mixed Provision</i>
<i>Private Goods</i>	Clothes, Food, Cars, Private Housing	Food Supply as in Communist China in the End of 1950s	Transportation, Medical Care
<i>Public Goods</i>	Foreign Aid	National Defense	Pollution Reduction

owners, and, therefore, everybody is in a worse situation than would be if everyone provided the security that would have spillover benefits for everyone else.

As we have seen, cybersecurity is both excludable and rivalrous. Cybersecurity has neither territorial boundary nor industrial limit. In the global village, all individuals and organizations are confronted with risks of the same level. In this environment, the security of individuals or organizations' systems matters firstly to themselves. Only in some accidental situations are others involved, such as in the case of DOS attacks.

Powell provides evidence from the financial services industry to prove that cybersecurity is hardly a public good.²⁰ Individuals and organizations have excludability in cybersecurity. The excludability of cybersecurity roots in the three characteristics of cybersecurity, i.e., confidentiality, integrity and availability, among which confidentiality fully expresses the excludability of cybersecurity. We could see the situation this way: if security is available to one user, it is unavailable to other users, and if others enjoy security, ones' security does not exist any longer. Unsurprisingly, cybersecurity is characterized as preservation of confidentiality, ensuring that information is accessible only to those authorized to have access; integrity, safeguarding the accuracy and completeness of information and processing methods; availability, ensuring that authorized users have access to information and associated assets when required. The users' security is enjoyed solely by themselves. Any sharing entails that systems become insecure. In fact, hackers are precisely the exploiters and sharers of insecure systems. Therefore, cybersecurity has more excludability than any private good.

On the other hand, the cost of expanding security to others is not zero, but enormously high. If one user enjoys a higher level of security, the level of security of the others will relatively decrease. As mentioned above, there is no perfect security. Security and insecurity are relative concepts that exist in comparisons. If one enjoys a higher level of cybersecurity, the level of security of the others will decrease to insecurity. The competition between the security measures is the reason that causes increase of the difference between the relative securities. Of course, the enhancement of the total security level benefits from that competition.

Katyal's study stresses that to some extent private security measures may increase crime.²¹ The basic assumption behind this argument is that, if one household locks its door, the thief will turn to the neighbor whose doors are left unlocked. Therefore, locking of one's own door breaks the reciprocity and mutual trust in the neighborhood. If we consider the fact that currently nearly all households, companies, and even government agencies "lock their own doors," we can easily conclude that this assumption is absurd. Only when every household, company and governmental agency is convinced not to take such "inefficient" measures is such an assumption significant. The author believes that such an assumption ignores the dual value of locking in the prevention of crime: on one hand, locking protects from damage and harm, making the potential criminals shrink back at the sight, or taking criminals more time before suffering losses; on the other hand, locking increases the potential criminals' time consumption and material costs in looking for new victims, and even making it impossible for them to find one. If none of the households and organizations locks their doors, potential criminals can easily find possible targets. Therefore, the difficulty of crime will decrease, and the efficiency will increase. The potential criminals are indifferent about costs, benefits, likelihood of success.

This pertains particularly to cybersecurity. If every computer owner is encouraged not to use security control, the computer will be more vulnerable to attacks. Assuming that the environment and the potential of all individual and organizations' computers are the same and the risk of being attacked is also approximately similar, then only when the benefits related to cybersecurity are equal could the provision of public cybersecurity be efficient. But this situation rarely exists in reality. Therefore, an unlimited public cybersecurity would be excessive for some individuals and organizations and insufficient for others. The situation of abundance is economically inefficient, while the situation of insufficiency is inefficient in terms of security. Hence, both ways, the public cybersecurity control cannot function optimally. In result, if cybersecurity is provided in the mode of public good, it is impossible to be more beneficial than as a private good.

Kobayashi notes that cybersecurity is different from traditional security.²² To discourage crime *ex ante* in the general criminal context, the government could implement sufficient level of punishment to deter the crime from accruing. In the case of cybercrime, the likelihood of detecting is so low that the penalty imposed would have to be of considerable magnitude to deter cybercrime. In what follows, the author will explore the possibility of establishing liability for the different participants in the process of cybersecurity provision.

Public Provision of Cybersecurity: Liability Mechanisms

Even if it were technically feasible to keep all systems 100% secure, the costs would have been so prohibitive as to render such an approach an economic prescription for disaster. The government can neither provide cybersecurity nor manipulate the systems. Naturally, one of the Ernst & Young survey's key findings was that only 11% deemed government security-driven regulations as being highly effective in improving their information security posture or in reducing data protection risks.²³ However, any argument stating that the governments can play no role in the field of cybersecurity is over skeptical. The governments can play a necessary role in deterring the attackers, but they are by no means helpless in the maintenance of an adequate level of cybersecurity. Their roles are to impose penalty through legislation and deter crime by means of *ex post* law enforcement. Providing cybersecurity as a public good is confronted with greater difficulties in international cooperation than as a private good. Even if some countries can convince their taxpayers to pay for the expenses involved in the public provision of cybersecurity, if you cannot simultaneously convince all countries to do so, it will not be cost-efficient. In this section, the author will analyze the characteristics of the possible liability of various players in the field of cybersecurity.

Liability of Hackers

Ballon argues that the major benefits of holding the hacker liable for the damage he causes is that the target has more choices and control in applying the law against hackers.²⁴ Compared to a criminal action, the liability of hackers can be justified by that it grants the plaintiff "greater control over the litigation and potentially better long-term relief;" that it encourages attack reporting;²⁵ and that a target will have the motive to recover losses at the same time of punishing the perpetrator.²⁶

The disadvantage of tort liability of hackers lies in two aspects: on one hand, the plaintiff has to pay a significant amount of money before receiving any compensation; on the other hand, most hackers have had and will have greater incentives to be judgment-proof.²⁷ If a hacker has little to lose under tort liability mechanism, his most rational choice will be to hide more secretly himself and his assets.²⁸ In the networked world, tracking a hacker or finding his money will need more energy, time, and costs, and will even prove to be an impossible task. As a result, the hacker would carry out the act more judgment-proof. Even worse, the hacker might be forced by the civil actions to commit other money-harvesting offences to support his actions.

Currently, dozens of countries have enacted domestic law against cybercrime. In addition, there have also been successful international legal actions, such as the Convention on Cybercrime (2001) and other domestic provisions.²⁹ Although the legisla-

tion is already there, the practical effects are doubtful. There are many hackers but the detection probability is quite low and the application of legislation is rare.

Liability of Internet Service Providers

Internet Service Providers (ISP)'s tort liability plays an important role in the following two cases: first, a lower level of ISP's security standard might be exploited by hackers; and second, the ISP's vicarious liability for its employee's security breach makes it easier to recover the target's losses.³⁰ To justify the first aspect, an important economic consideration is that the ISP's cost to improve its security level is lower compared to the hackers' high potential cost to society, and with the security standard the security condition becomes more certain and reliable.³¹ This would be expected to lower the overall cost of the Internet service, provide incentive for Internet participation, and increase the value of the network to society.³² There is no theoretical obstacle in applying the tort liability to cybersecurity breaches.

The only problems in applying tort liability to all ISPs is that there is no uniform standard; that it would be difficult to provide such a standard; and that dual or multiple standard would surely motivate some ISPs to maintain a lower level of security due to economic reasons. The result of this dilemma will be that no deterrence functions on hackers.

Liability of Security Problems Publishers

The security (holes) publisher has two aspects of gain from the publication, one is that the publication can prevent some harm suffered by the general public, the other is that the publication realises more economic or other benefits. However, it takes great risk resulting in users' losses in case hackers exploit the publicized loopholes. In addition, the users have to invest in improving their security protection when they know the new publicized loopholes.

According to Coarse's general principle,³³ whether the publisher should be held liable for his publication is a question of whether the gain of both the general public users from stopping the potential harm and the publisher himself from obtaining a higher confidence value is greater than the losses that the users suffer from the attacks launched exploiting the publicized loopholes and from the extra investment in preventing such attacks. In different cases, the cost effectiveness is different, and is hard to prove. Finally, as Preston and Lefton put it:

The question is not whether an individual publication causes more harm than good; it is whether a particular rule of liability governing computer security publications causes more harm than good.³⁴

Liability of Security Providers

The rapid growth of the computer security industry leads people to consider whether security providers should be held liable when their products and services fail to protect against hackers. Developing higher security level of products and providing high security level of services are costly, but work to prevent hacking from taking place. Security providers' liability will create incentives for them to provide products or services of at least a standard level. The products and services containing security holes take great risks of product liability if their advertisements stated that they are "hack-proof."³⁵

The problem with holding security providers liable is that goods and services are usually provided subject to contract or licensing agreements, making tort liability inappropriate because the parties have bargained to allocate the risk between them.³⁶ The reasonable way in which the agreements are concluded is that neither of the two parties wants to bear more risk. But in general, the party of product or service users might have the greater discretion in choosing with more guarantees and less expenses. The security providers will be generally worse-off.

Liability of Software Vendors

Most of the security holes come from the bad design of software (and sometimes hardware). The software vendors control the only key to solve this problem through fixing their software. However, this work also consumes human resources and investments in terms of money. Therefore, vendors generally do not have the incentive to do so. A way to incorporate their better work into their best interests is to raise the risk of liability, which will raise the cost of their products. If software vendors have liability costs, they will pass those on to users. In turn, the vendors might as well pay to fix the problems.

Liability of Software Authors

Since the authors of software (the programmers) have the biggest opportunity to prevent problems, it seems appropriate to focus on making them responsible for the security of their products.³⁷ Nonetheless, there are some unique aspects of computer software that make it challenging to apply traditional notions of product liability.

Under such circumstances, if we impose liability on the authors, it is impossible, because the author gets no income to pay the compensation; it is inefficient, because the author would be discouraged from contributing; and it is also unfair, because the users use the software for free and voluntarily.

Liability of System Owners

Systems can be both targets and tools in attacks. For example in a Distributed Denial of Service attack, the attacks are launched from numerous manipulated computers. The owners of such systems, who use software written and sold by third parties, cannot fully secure their systems, cannot stop unforeseeable outsiders' exploitation, and have no way to reduce the risks. In order to hold the system owners liable, two prerequisites are necessary to be in place: the establishment of a security standard, and the mechanism of insurance. The latter was discussed by Fisk in analogy to vehicle operators who are often legally required to carry insurance against accidents.³⁸

Conclusion

This article argues that cybersecurity is a private good and should be provided mainly by the private sector. Regarding cybersecurity as a public good would discourage the private sector to invest in security provision. From this standpoint, an early government intervention would reduce the effectiveness and efficiency of cybersecurity. However, in terms of prevention of security breaches, law enforcement can play an important role in establishing and enforcing liability mechanisms. Although it is still controversial whether and how cybersecurity players should be held liable for their activities, every step made in this direction will bring benefits to the private sector to achieve their goals.

Acknowledgement

The author wishes to express his appreciation to Jenny and Antti Wihuri Foundation, the Department of Law at the University of Joensuu, and the Finnish Cultural Foundation, for their generous financial support for his current research. He also wishes to thank the Finnish Economic Education Foundation for supporting him in the early stage of this research. Certainly, the responsibility for the contents is the author's.

Notes:

- ¹ National Research Council, *Cryptography's Role in Securing the Information Society* (Washington, DC: National Academy Press, 1996).
- ² John McCormick, "Five Reasons You're not Secure," 5 April 2005, <insight.zdnet.co.uk/internet/security/0,39020457,39193819,00.htm> (14 Dec. 2005).
- ³ Dan Farmer, "Shall We Dust Moscow?: Security Survey of Key Internet Hosts & Various Semi-Relevant Reflections," November-December 1996, <<http://www.trouble.org/survey/>> (14 Dec. 2005).
- ⁴ Jennifer A. Chandler, "Security in Cyberspace: Combating Distributed Denial of Service Attacks," *University of Ottawa Law & Technology Journal* 1 (2003-2004): 231-261, <<http://www.uoltj.ca/articles/vol1.1-2/2003-2004.1.1-2.uoltj.Chandler.231-261.pdf>> (14 Dec. 2005).
- ⁵ Christopher Coyne and Peter Leeson, "Who Protects Cyberspace?" Working Paper 24 (George Mason University, Department of Economics, Global Prosperity Initiative, 2004), <<http://www.mercatus.org/pdf/materials/616.pdf>> (14 Dec. 2005).
- ⁶ Benjamin Powell, "Is Cybersecurity a Public Good? Evidence from the Financial Services Industry," Working Paper Number 57 (The Independent Institute, 15 March 2001), <http://www.independent.org/pdf/working_papers/57_cyber.pdf> (14 Dec. 2005).
- ⁷ Torgeir Daler, Roar Gulbrandsen, Birger Melgrd, and Torbjorn Sjølstad, *Security of Information and Data* (Ellis Horwood, January 1989), 15.
- ⁸ Lawrence A. Gordon, Martin P. Loeb, William Lucyshyn, and Robert Richasrdson, *Tenth Annual CSI/FBI Computer Crime and Security Survey* (Computer Security Institute, 2005), 11, <http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2005.pdf> (14 Dec. 2005).
- ⁹ CERT Coordination Center, *CERT/CC Statistics 1988-2005* (2005), <http://www.cert.org/stats/cert_stats.html> (14 Dec. 2005).
- ¹⁰ Peter G. Neumann, "Information System Adversities and Risks" (paper presented at the Conference on International Cooperation to Combat Cyber Crime and Terrorism, Stanford, CA: Hoover Institution, 1999).
- ¹¹ Carl Howe, John C. McCarthy, Tom Buss, and Ashley Davis, "The Forrester Report: Economics of Security," (February 1998).
- ¹² Gordon, Loeb, Lucyshyn, and Richasrdson, *Tenth Annual CSI/FBI Computer Crime and Security Survey*, 15.
- ¹³ Stephen J. Lukasik, "Protecting the Global Information Commons," *Telecommunication Policy* 24, no. 6-7 (2000): 519-531.
- ¹⁴ Robert L. Ullman and David L. Ferrera, "Crime on the Internet," *Boston Bar Journal*, no. 6 (November/December 1998).
- ¹⁵ L. Jean Camp and Catherine Wolfram, "Pricing Security," in *Proceedings of the CERT Information Survivability Workshop* (Boston, Massachusetts, 24-26 October 2000), 31-39, <www.ljean.com/files/isw.pdf> (14 Dec. 2005).
- ¹⁶ Camp and Wolfram, "Pricing Security."
- ¹⁷ Source: "Good (Economics and Accounting)," Wikipedia, the free encyclopedia <http://en.wikipedia.org/wiki/Good_%28economics%29> (15 Dec. 2005).

¹⁸ Paul A. Samuelson, "The Pure Theory of Public Expenditure," *Review of Economics and Statistics* 36 (November 1954): 387-389.

¹⁹ Hal R. Varian, "System Reliability and Free Riding," in *Proceedings of the First Workshop on Economics and Information Security* (University of California, Berkeley, 16-17 May 2002), <<http://www.sims.berkeley.edu/resources/affiliates/workshops/econsecurity/econws/49.pdf>> (14 Dec. 2005).

²⁰ Powell, "Is Cybersecurity a Public Good? Evidence from the Financial Services Industry."

²¹ Neal Kumar Katyal, "The Dark Side of Private Ordering for Cybersecurity," in *The Law and Economics of Cybersecurity*, ed. Mark F. Grady and Francesco Parisi (Cambridge University Press, November 2005).

²² Bruce H. Kobayashi, "An Economic Analysis of the Private and Social Costs of the Provision of Cybersecurity and Other Public Security Goods," *Supreme Court Economic Review* 14 (2005), <<http://law.bepress.com/gmulwps/gmule/art26>> (15 Dec. 2005).

²³ Earnest & Young, *Global Information Security Survey 2004*, BYG No. FF0231, <[http://www.ey.com/global/download.nsf/International/2004_Global_Information_Security_Survey/\\$file/2004_Global_Information_Security_Survey_2004.pdf](http://www.ey.com/global/download.nsf/International/2004_Global_Information_Security_Survey/$file/2004_Global_Information_Security_Survey_2004.pdf)> (14 Dec. 2005).

²⁴ Ian C. Ballon, "Alternative Corporate Responses to Internet Data Theft," in *17th Annual Institute on Computer Law* 737, 744 (PLI Patents, Copyrights, Trademarks & Literary Prop. Course, Handbook Series No. 471, 1997).

²⁵ David L. Gripman, "The Doors Are Locked but the Thieves and Vandals Are Still Getting in: A Proposal in Tort to Alleviate Corporate America's Cyber-Crime Problem," *16 J. Marshall J. Computer & Information Law*, 167 (1997): 174-176.

²⁶ Michael Hatcher, Jay McDannel, and Stacy Ostfeld, "Computer Crimes," *American Criminal Law Review* 36, 397 (1999): 406.

²⁷ James Brooke, "Calm Scene Isn't Really, Police Say," *New York Times*, 22 April 2000, C1.

²⁸ Mary M. Calkins, "They Shoot Trojan Horses, Don't They? An Economic Analysis of Anti-Hacking Regulatory Models," *Georgia Law Journal* 89, no. 171 (November 2000): 214-217.

²⁹ Convention on Cybercrime 2001.

³⁰ David Icove, Karl Seger, and William VonStorch, *Computer Crime: A Crimefighter's Handbook* (O'Reilly and Associates, Inc., August 1995): 427.

³¹ Icove, Seger, and VonStorch, *Computer Crime*.

³² Marc D. Goodman, "Why the Police Don't Care about Computer Crime," *Harvard Journal of Law and Technology* 10, no. 3 (1997): 465-494.

³³ Ronald H. Coase, "The Problem of Social Cost," *Journal of Law and Economics* 3 (1960): 1-44.

³⁴ Ethan M. Preston and John Lofton, "Computer Security Publications: Information Economics, Shifting Liability and the First Amendment," *Whither Law Review* 24, no. 71 (Fall 2002): 130.

³⁵ Natalee Drummond and Damon J. McClendon, "Cybercrime – Alternative Models for Dealing with Unauthorized Use and Abuse of Computer Networks," (Summer 2001), <http://gsulaw.gsu.edu/lawand/papers/su01/drummond_mcclendon/> (14 Dec. 2005).

³⁶ E. Gabriel Perle, Mark A. Fischer, and John Taylor Williams, "Electronic Publishing and Software," Part A, *Computer Law* (January 2000).

³⁷ Mike Fisk, “Causes and Remedies for Social Acceptance of Network Insecurity” (paper presented at Workshop on Economics and Internet Security, University of California, Berkeley, 16-17 May 2002), 3, <<http://www.sims.berkeley.edu:8000/resources/affiliates/workshops/econsecurity/econws/35.pdf>> (14 Dec. 2005).

³⁸ Fisk, “Causes and Remedies for Social Acceptance of Network Insecurity.”

XINGAN LI, born in 1967, LLB (1989), LLM (1994), is Associate Professor at Inner Mongolia University Law School. He was a visiting scholar at Kyushu University (2000-2001), and researcher at the University of Lapland and the University of Joensuu. His research interests are criminology, criminal psychology, criminal law and criminal procedural law, and particularly, cybersecurity and cybercrime. His publications include the books “Criminal Law of England and Wales,” “Principles of Criminal Law,” and several papers on economic crime, cybersecurity and cybercrime. *Address for Correspondence:* Sepänkatu 15 C 57, 80110 Joensuu, Finland; *Phone:* +358 044 910 7632; *E-mail:* li@cc.joensuu.fi.

The Criminal Phenomenon on the Internet: Hallmarks of Criminals and Victims Revisited through Typical Cases Prosecuted

Xingan Li *

WITH THE GROWTH OF RESEARCH ON CYBERCRIME, increased attention has been given to the hallmarks of cybercriminals and the security levels of cybervictims by lawyers and law enforcement officials. The purpose of this study is to present an updated profile of cybercriminality and cybervictimization based on empirical methods. The study uses a sample of 115 typical cases prosecuted between 18 March 1998 and 12 May 2006, which were published on the official website of the United States Department of Justice. The study found that males are responsible for a majority of these cybercrimes. Cybercriminals are primarily between the ages of 17 and 45. Domestic perpetrators constitute the absolute majority of the cybercriminals. Outsiders are four times more likely to be involved in cybercrimes than insiders. Most cybercrimes did not involve monetary loss, while those that did caused an average of one million dollars in damage. The most vulnerable interests are in the private sector. The security measures taken by victims are surprisingly weak, and are vulnerable to uncomplicated cybercrimes. The punishments (both imprisonment and fines) for cybercrime are generally light.

AVEC L'ESSOR DE LA RECHERCHE SUR LA CYBERCRIMINALITÉ, les avocats et les responsables de l'application des lois accordent une attention accrue sur les indices des cybercriminels et des niveaux de sécurité des victimes de la cybercriminalité. L'objectif de cette étude consiste à présenter une mise à jour de la cybercriminalité et de la « cybervictimisation » fondée sur des méthodes empiriques. L'étude se sert d'un échantillonnage de 115 cas typiques ayant fait l'objet de poursuites entre le 18 mars 1998 et le 12 mai 2006, publiés sur le site Web officiel du Department of Justice des États-Unis. Selon cette étude, la majorité des cybercrimes sont commis par des hommes. L'âge des cybercriminels se situe en général entre 17 et 45 ans. Les contrevenants à l'échelon national constituent la majorité absolue des cybercriminels. Les contrevenants externes à l'organisation ont quatre fois plus de chance d'être impliqués dans des cybercrimes que les gens de l'intérieur. Les plupart des cybercrimes ne portaient pas sur des pertes d'argent, quoique ces crimes eussent entraîné des pertes moyennes d'un million de dollars. Les intérêts les plus vulnérables se retrouvent dans le secteur privé. Les mesures prises par les victimes pour assurer leur sécurité sont étonnamment faibles et exposées à des cybercrimes simples. Les sanctions (les peines d'emprisonnement et les amendes) imposées en cas de cybercrime sont en général assez légères.

127	1. INTRODUCTION
128	2. LITERATURE REVIEW
132	3. METHODS
132	4. RESULTS
132	4.1. <i>Gender Distribution of Cybercrime</i>
132	4.2. <i>Age Distribution of Cybercrime</i>
133	4.3. <i>Domestic Versus Foreign Perpetrators</i>
133	4.4. <i>Insider Versus Outsider</i>
134	4.5. <i>Losses Resulting From Cybercrime</i>
134	4.6. <i>Victims of Cybercrime</i>
134	4.7. <i>Security Level of the Victim</i>
135	4.8. <i>Complexity of Cybercrime</i>
135	4.9. <i>Imprisonment Sentences</i>
135	4.10. <i>Fines</i>
136	5. DISCUSSION AND CONCLUSION

The Criminal Phenomenon on the Internet: Hallmarks of Criminals and Victims Revisited through Typical Cases Prosecuted

Xingan Li

1. INTRODUCTION

THE SOCIAL CHANGES OF RECENT DECADES HAVE BEEN PRIMARILY driven by the development of information and communications technology. One of the most significant negative impacts in this context is the emergence and rampancy of cybercrime. Research on criminal activity related to information and communications technology has become a focus of study in the fields of criminology, criminal law and information security.

Cybercrime is a comprehensive topic and attracts scholars from different disciplines. Many have written about the theoretical explanation for cybercrime. Studies of cybercrime have revealed different dimensions of this phenomenon. While the limited previous first-hand explorations have been widely accepted and cited, inconsistencies exist among various studies. Unfortunately, in the field of cybercriminal and cybervictim profiling, most subsequent theoretical treatises tend to reinforce the earliest findings, or at most provide some modest revisions.

It is critical to answer the following questions: Who is most likely to commit cybercrime? Who is most likely to be victimized by cybercrime? And what are the similarities between cybercrime perpetrators and their victims? The subject of cybercrime leads the tide of the theory and practice of legislation and law enforcement in the sense that the perpetrators are those who challenge the traditional legal system. Studies on the subject of computer crime have a history of several decades and have established widely-accepted profiles for cybercriminals and their victims.

With the deepening of the research on cybercrime, lawyers and law enforcement officials are paying increased attention to the hallmarks of cybercriminals and the security of cybervictims. The purpose of this study is to present an updated profile of cybercriminality and cybervictimization, through the analysis of 115 typical cybercrime cases prosecuted in the United States of America between 18 March 1998 and 12 May 2006, and published on the Department of Justice website.

*

2. LITERATURE REVIEW

WHEN WE TALK ABOUT SUBJECTS OF CYBERCRIME, we are referring to the profile of the perpetrators of these crimes. However, the cybercriminal is not one single person, but represents a class of perpetrators. Previous literature has focused on who is most likely to commit cybercrime and who is most likely to be a victim of cybercrime. Any conclusions drawn from the hundreds or thousands of cases might be premature or even misleading. More than 20 years ago, Bequai pointed out that no one single profile could be developed of a cybercriminal.¹ Bequai offered a tentative profile of the typical perpetrator of computer crime based on hundreds of cases compiled from statistics by the United States Bureau of Justice.² Like many scholars, he was worried that attempts to oversimplify the profile of cybercriminals could have a misleading effect on our understanding of cybercrime. Bequai states that:

Studies of computer criminals usually portray them as young, educated, technically competent, and usually aggressive. Some steal for personal gain, others for the challenge, and still others because they are pawns in a larger scheme. ... Still other studies typically portray computer criminals as technicians, managers, and programmers. They are usually perceived as jovially challenging the machine, and discovery occurs only through inadvertence. ... The theft usually involves money, services, or trade secrets. However, when caught, the computer criminal's sentence is light compared to that of traditional property-crime felons, who usually receive harsh sentences for crimes involving much less property or money.³

It is widely recognized that there is no single profile that can "capture the characteristics of a 'typical' computer criminal, and many who fit the profile are not [necessarily] criminals at all."⁴ Donn B Parker presented a brilliant portrait of a perpetrator of computer crime, stating that "[p]erpetrators are usually bright, eager, highly motivated, courageous, adventuresome, and qualified people willing to accept a technical challenge. They have exactly the characteristics that make them highly desirable employees in data processing."⁵

The development of computer technology has changed this depiction completely.⁶ Becker suggested seven views of computer systems: the playpen, the land of opportunity, the cookie jar, the war zone, the soapbox, the fairyland, and the toolbox.⁷ Bequai researched how the potential sources of computer attack might vary from one to another, and found that the majority of perpetrators could essentially be grouped into three categories: dishonest insiders; outsiders; and users.⁸ This implied that everyone had an equal chance of being involved in

1. August Bequai, *How to Prevent Computer Crime: A Guide for Managers* (John Wiley & Sons., 1983) at p. xviii.
2. Bequai, *How to Prevent*, *supra* note 1 at pp. 42-45.
3. August Bequai, *Computer Crime* (Lexington Books, 1978) at p. 4.
4. Charles P Pfleeger and Shari Lawrence Pfleeger, *Security in Computing*, 3d ed., (Prentice Hall, 2003) at p. 20.
5. Donn B Parker, *Crime by Computer* (Charles Scribner's Sons, 1976) at p. 45.
6. Jay Becker, "Who are the Computer Criminals," (1981) 25:1 *Security Management* 18-22.
7. Becker, "Computer Criminals," *supra* note 6 at pp. 18-20.
8. Bequai, *How to Prevent*, *supra* note 1 at pp. 47-50.

computer crime, at a time when the internet was not as widespread as it is presently. Wasik concentrated on the characteristics and classifications of perpetrators as well.⁹ Levinson sorted categories of cyber threats into five groups: insiders, hackers, virus writers, criminal groups, and terrorists.¹⁰ Reynolds classified perpetrators into hacker, cracker, insider, industrial spy, cybercriminal and cyberterrorist.¹¹ That is to say, the widespread use of computers created a multi-dimensional social environment that allowed potential computer criminals to discover new opportunities for attack.

Internet users worldwide are strongly sex divided; that is, a higher percentage of males than females use the internet. For example, in 2001, women made up 6 percent of internet users in the Arab states, 38 percent in Latin America, 25 percent in the EU, 37 percent in China, 19 percent in Russia, 18 percent in Japan, 17 percent in South Africa, and nearly 50 percent in the United States.¹² However, the gender gap is narrowing, with females constituting the majority of internet users in some countries. In Nordic countries, it was found that men constitute a higher percentage of daily users of the internet than women.¹³ Previous studies showed that cybercrime is far more sex divided than internet use. According to Levinson, "[i]t is well established that boys commit far more juvenile crime, particularly violent crime, than girls."¹⁴ Cybercrime seems less violent, but the research indicates that more males commit cybercrimes than females. According to Jiang, males constitute 91.45 percent of the perpetrators, while females constitute only 8.55 percent.¹⁵ He suggested that this was the result of differences between males and females in computer knowledge and skills combined with attitudes in online interactions. However, the reasons why females are found guilty of cybercrime less often than males are not clear at all. Specific research is needed to address the following questions: Do women commit less cybercrime? Are cybercrimes committed by women less likely to be detected? More philosophically, can we measure this criminal phenomenon among men and women using the same concept? But this study is not intended to answer these questions.

A noteworthy phenomenon is that whether it be individual cybercrime, corporate cybercrime, or organized cybercrime, young perpetrators play a critical part. Although there is no age limit to commit cybercrime, we found that, similar to traditional crimes, youth constitute an important proportion of the cybercriminals. As LR Shannon reported, in 1993, cybercriminals tend to be between the ages of 14 and 30; they are usually bright, eager, highly motivated, adventuresome and willing to accept technical challenges.¹⁶ The age of criminal responsibility varies from nation to nation. In most countries, children younger

9. Martin Wasik, *Crime and the Computer* (Oxford University Press 1991) at pp. 60-65.
10. David Levinson, ed., *Encyclopedia of Crime and Punishment*, vol. 2. (Sage Publications, 2002) at p. 525.
11. George Reynolds, *Ethics in Information Technology* (Thomson Course Technology 2003) at pp. 58-65.
12. Women's Learning Partnership, "Technology Facts & Figures," (December 2001), <http://www.learningpartnership.org/resources/facts/technology>.
13. Nordic Council of Ministers, "Nordic Information Society Statistics 2005," Report, <http://www.norden.org/pub/uddannelselse/IT/IT2005562.pdf> at p. 42.
14. Levinson, *Encyclopedia*, *supra* note 10 at p. 490.
15. Ping Jiang, *A Study of Computer Crime* (Shang wu yin shu guan, 2000) at pp. 151-152.
16. LR Shannon, "The Happy Hacker," review of Paul Mungo and Bryan Clough, *Approaching Zero: The Extraordinary Underworld of Hackers, Phreakers, Virus Writers, and Keyboard Criminals* (Random House, 1993), (21 March 1993) *The New York Times* G 16, <http://query.nytimes.com/gst/fullpage.html?res=9F0CE1D71E3BF932A15750C0A965958260>.

than 14 or 15 years of age are not liable for criminal offences, while children between 15-17 or 14-16 years of age are liable for a limited range of offences.¹⁷ In fact, juveniles commit a number of these crimes. In China, individuals between the ages of 19 and 40 make up 80 percent of all internet users, and the average age of cybercrime perpetrators is 23.¹⁸ Juvenile delinquency and juvenile justice have become issues closely associated with cybercrime. According to findings of criminal psychological research, the reason why children are more likely to commit crime is not because more and more children will commit crime, but because most of the potential offenders will commence to commit crime in childhood and continue their criminality for much of their lifetime. After 16-17 years of age, the offending rates decreases to a plateau.¹⁹

Underwood found that cybercriminal behaviour cuts across a broad range of society, with the age of most offenders ranging from 10 to 60 years.²⁰ People between the ages of 20 and 59 make up 94 percent of computer criminals, with the most active being people in their thirties.²¹

Bequai's profile of typical computer criminal presented a full portrait of the above mentioned features, with other aspects.²² He stated that the age of computer criminals is between 15 and 45 years old. He found that males were responsible for most computer crimes, but that the proportion committed by females was increasing. The occupational experience of computer criminals ranged from the highly experienced technician to the minimally experienced professional. Both public and private sectors could be victims of computer crimes. Computer criminals had the personal traits of being bright, motivated, and ready to accept technical challenges. They were usually desirable employees who were hard and committed workers. Computer crimes were mostly committed by individuals, but conspiracies were increasing. Most offences were committed by insiders who had easy access to the computer system. The security of the victims' system was usually lax.

An important topic of research has been the distinction between the sources of offenders and the relationship between offenders and their victims, which can be used to divide offences into those committed by insiders and those committed by outsiders. Shaw, Ruby and Post classified insiders into information technology specialists such as full-time or part-time employees, contractors, consultants, or temporary workers; partners and customers with system access; and former employees retaining system access.²³ There have been different findings as to whether insiders or outsiders constitute the greatest threat to computer system security.²⁴

17. For example, in Article 17 of the penal law of China, children under 14 years old of age are not liable; in Section 4, Chapter 3 of the Penal Code of Finland, <<http://www.finlex.fi/pdf/saadkaan/E8890039.PDF>>, the age limit is 15. In some other countries, the liability age is even lower. In England and Wales, the age is 10-year-old, while the limited liability ages are between 10-14 years of age.
18. B Dong, "Eighty Percent of Net Café Consumers are Youths," (15 October 2003) *China Youth Newspaper*
19. Dennis Howitt, *Forensic and Criminal Psychology* (Prentice Hall, 2002) at pp. 76-77.
20. Jim Underwood, "Criminal Profile," (1999), <<http://www-staff.its.uts.edu.au/~jim/cit2/cit2-99/legal/CrimProf.html>>
21. Jim Underwood, "Criminal Profile," *supra* note 20.
22. Bequai, *How to Prevent*, *supra* note 1 at p. 43.
23. Eric D Shaw, Keven G Ruby, and Jerrold M Post, "The Insider Threat to Information Systems," (1998) 2-98 *Security Awareness Bulletin*, <<http://rf-web.tamu.edu/security/secguide/Treason/InfoSys.htm>>.
24. For example, The AFCOM's Data Centre Institute found that the cyber attacks launched by outsiders (52 percent) were ten times that of the insiders (5 percent). However, the respondents were more concerned the insider threats than the outsider ones. See Edward Hurley, "Are Insiders Really a Bigger Threat?" (17 July 2003), <http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci906437,00.html>.

Mainstream findings support the view that insiders are more likely to be involved in computer crimes against the employers' systems. The Nordic Council of Ministers found that students, employees and self-employed people constitute the highest percentage of internet users.²⁵ Mackenzie and Goldman reported that "some students, particularly computer science and engineering majors, with newly discovered skills attempt to break into the servers" of University of Delaware.²⁶ In November 2003, Meta Group found that, of more than 1,600 information and communications technology professionals, current employees represent the biggest threat to technology infrastructures.²⁷ The Computer Security Institute and Federal Bureau of Investigation found that 55 percent of survey respondents reported malicious activity by insiders.²⁸ Researchers also revealed that dissatisfied employees are a major source of computer crimes²⁹ and are the greatest threat to a computer's security.³⁰ When Sutherland coined the term "white-collar crime" in the late 1930s, he could have hardly imagined that crimes would be committed in the process of human-machine interaction, in addition to human-human interaction, human-organization interaction, or human action against machines. Nevertheless, the term "white-collar cybercrime" was recently introduced as a contribution to develop Sutherland's theory.³¹

Besides the revealed relationship between criminals and victims, others have also explored the characteristics of victims. Debra Littlejohn Schinder suggests a summary of common cybervictim characteristics: they are new to the internet; naturally naïve; disabled or disadvantaged; greedy; lonely or emotionally needy; pseudo-victims in the sense that they may falsely report being victimized; or are simply unlucky enough to be in the wrong virtual place at the wrong time.³²

From the previous literature, the profile of the cybercriminal and the cybervictim can hardly be regarded as settled. In addition, the available literature does not provide detailed sources of materials nor does it clarify the methods used. Many studies have apparently been based on second-hand materials and mass media reports. There is still a need for findings about the hallmarks of cybercriminals and cybervictims drawn from the prosecuted cases.

25. "Nordic Information Society Statistics 2005," *supra* note 12 at p. 42.

26. Elizabeth MacKenzie and Kathryn Goldman, "Computer Abuse, Information Technology, and Judicial Affairs," in *Proceedings of the 28th Annual ACM SIGUCCS Conference on User Services: Building the Future* (ACM Press, 2000) 170-176 at p. 174.

27. Meta Group, "Security Spending Spree," (20 January 2004) 23:1 PC Magazine 25.

28. Bill Hancock, "Security Views," (1999) 18:3 Computers and Security 188-189.

29. Michael A Vatis (Director, National Infrastructure Protection Center, Federal Bureau of Investigation), Statement for the Record, *NIPC Cyber Threat Assessment*, hearing, Senate Judiciary Committee Subcommittee on Technology and Terrorism, 106th Congress, 1st session (USA, 6 October 1999) at "Insider Threat."

30. Eric J Sinrod and William P Reilly, "Cyber-Crimes: A Practical Approach to the Application of Federal Computer Crime Laws," (2000) 16:2 Santa Clara Computer and High Technology Law Journal 177-232 <<http://www.sinrodlaw.com/CyberCrime.pdf>>.

31. See for example, Victim Assistance Online, "White Collar Cybercrime," <http://www.vaonline.org/internet_wcollar.html>. The term "White-Collar Hacker" is also used, for example, by John Leyden, "The Rise of White Collar Hacker," (31 March 2004) *The Register*, <http://www.theregister.co.uk/2004/03/31/the_rise_of_the_white/>.

32. Debra Littlejohn Shinder, *Scene of the Cybercrime: Computer Forensics Handbook* (Syngress Publishing, 2002).

*

3. METHODS

THE STUDY USED A SAMPLE OF 115 TYPICAL CASES sentenced or on trial between 18 March 1998 and 12 May 2006 published on the website of the United States Department of Justice. The study took all the cases listed on the website of the United States Department of Justice Computer Crime & Intellectual Property. The webpage notes: "Below is a summary chart of recently prosecuted computer cases. Many cases have been prosecuted under the computer crime statute, 18 U.S.C. §1030 [(2000) 18 United States Code s. 1030, <http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=browse_usc&docid=Cite:+18USC1030>]. This listing is a representative sample; it is not exhaustive."³³

The study classified the sample cases as follows: hacking and illegal access; attack, sabotage and botnet; viruses, worms, spyware and logic bomb; data theft and espionage; ID theft and fraud; and miscellaneous, which includes embezzlement and corruption. The strict legal categorization is not used in this study. Rather, the classification is based on criminological characteristics of the behaviours.

The statistical items considered in this study include: the demographic characteristics of the cybercriminal (including gender, age, insider or outsider, American citizen or foreigner); the nature of the victims (including private, public, both private and public, and threat to public health or safety); the outcomes of the cases; the decided sentence for the cybercrime (imprisonment and fine), the level of security of the victim (classified into strong, medium, and weak); and the complexities of techniques involved (classified into complicated, medium, and simple).

*

4. RESULTS

4.1. Gender Distribution of Cybercrime

IN MOST CATEGORIES OF OFFENCES, MALE OFFENDERS constitute the absolute majority of the criminals. Only two female offenders are reported in hacking and illegal access and one female offender is reported in miscellaneous offences. Overall, male offenders constitute more than 98 percent of the total perpetrators, while females are less than two percent.

4.2. Age Distribution of Cybercrime

The report from the website is incomplete in providing offenders' age information in every category of offence. Age data is missing for 73.1 percent of ID theft offences; 30.4 percent of attack, sabotage and botnet offences; 18.2 percent of viruses, worms, spyware and logic bomb offences; 15.9 percent of hacking and illegal access offences; 14.3 percent of data theft and espionage offences; and 14.3 percent of miscellaneous offences.

33. United States Department of Justice, Computer Crime & Intellectual Property Section, "Computer Crime Cases," <<http://www.cybercrime.gov/cccases.html>>.

Three perpetrators younger than 16 years old were convicted of offences in the categories of hacking and illegal access, and viruses, worms, spyware and logic bomb.

Offenders in the age category older than 46 years old were found in all categories of offences, except for fraud and miscellaneous offences. Generally, offenders over the age of 46 years old are not active in computer crime and constitute a small percentage of the total reported offenders, including offences for which ages are not available. For example, offenders over the age of 46 years old were convicted for 28.6 percent of data theft and espionage offences; 9.1 percent of virus, worms, spyware and logic bomb offences; 4 percent of attack and sabotage offences; and 3.8 percent of ID theft offences.

Cybercriminals are primarily between the ages of 17 to 45 years old. Offenders in this age group committed 79.3 percent of crimes involving hacking and illegal access; 65.2 percent of those involving attack and sabotage; 63.7 percent of those involving viruses, worms, spyware and logic bombs; 85.8 percent involving data theft and espionage; 26.8 percent involving ID theft; 100 percent involving fraud; and 85.7 percent that can be categorized as miscellaneous.

A more detailed distribution of offenders between the ages of 17 and 45 years old can be described as follows: the number of the offenders between the ages of 17 and 25 is 41; the number between 26 and 35 is 39; and the number between 36 and 45 is 21. These categories constitute 27 percent, 26 percent, and 17 percent of all offenders respectively. In the age group of 17 to 45 years old, 17 to 25-year-olds constitute 40.6 percent; 26 to 35-year-olds 38.6 percent; and 36 to 45-year-olds 20.8 percent. The ratios of offenders seem to decrease with age.

4.3. Domestic Versus Foreign Perpetrators

Altogether 14 out of 115 cases, or less than 12.2 percent, were committed by international perpetrators or foreigners. Domestic perpetrators are responsible for the remaining 87.8 percent of cybercrimes. The majority of reported cases are domestic computer offences.

4.4. Insider Versus Outsider

Insiders and outsiders constitute different ratios in different categories of offences. Insiders constituted the majority of offenders for offences of data theft, espionage, and fraud.

The categories in which outsiders constitute the majority of offenders include: exactly 100 percent of ID theft offences; 92.9 percent of miscellaneous offences; 87 percent of attack, sabotage and botnet offences; 81.8 percent of viruses, worms, spyware and logic bomb offences; and 76.2 percent of hacking and illegal access offences. Outsiders also constitute a strong ratio of 42.9 percent in fraud offences.

Former employees are included in the category of outsiders. Former employees make up 43.5 percent of offenders of attack and sabotage. They also constitute 12.7 percent of offenders of hacking and illegal access, and 7.2 percent of offenders of miscellaneous offences.

Overall, insiders and outsiders constitute 21 percent and 79 percent of all reported offenders respectively. Former employees constitute 16 percent of all of the outsiders. If former employees are added to insiders, they would constitute about 34 percent of the total offenders, still a smaller ratio than outsiders.

4.5. Losses Resulting From Cybercrime

In more than 59 percent of cybercrime cases, no loss was mentioned in the report. Among the remaining 41 percent of cases, 7 percent report losses of less than 10,000 dollars; 15.7 percent report losses between 10,000 and 100,000; 10.4 percent report losses between 100,000 and one million dollars; and 9.6 percent report losses of more than one million dollars.

The cybercrime offences with the greatest losses were hacking and illegal access; viruses, worms, spyware and logic bomb; ID theft; and miscellaneous offences, each resulting in losses of over one million dollars. The average losses resulting from attack and sabotage, data theft and espionage, and fraud are relatively lower: USA\$160,000, USA\$5,000 and USA\$384,000, respectively.

Overall, the average loss of the reported 49 cases is USA\$2.989 million. Adding cases without losses reported, the average loss still reaches USA\$1.274 million.

4.6. Victims of Cybercrime

The private sector is the primary victim of cybercrime. All of the cases of data theft and espionage, ID theft, and fraud are against private interests. 87.5 percent of miscellaneous offences, 81.8 percent of viruses, worms, spyware and logic bomb offences, 77.3 percent of attack and sabotage offences, and 69.5 percent of hacking and illegal access offences are committed against the private sector.

Only 18.2 percent of attack and sabotage offences, 13.6 percent of hacking and illegal access offences, and 12.5 percent of miscellaneous offences are committed against the public sector. However, 15.3 percent of hacking and illegal access cases and 9.1 percent of viruses, worms, spyware and logic bomb cases are against both private and public sectors.

In addition, 9.1 percent of viruses, worms, spyware and logic bomb cases, 4.5 percent of attack and sabotage cases, and 1.7 percent of hacking and illegal access cases are against public health and safety interests.

4.7. Security Level of the Victim

In the majority of cases, security is weak. Exactly 100 percent of cases of data theft and espionage and ID theft are possibly due to the absence of appropriate security. In other cases, 90.9 percent of viruses, worms, spyware and logic bomb cases, 87.5 percent of miscellaneous cases (including embezzlement and corruption), 82.6 percent of attack and sabotage cases, 80 percent of fraud cases, and 74.6 percent of hacking and illegal access cases are due to weak security.

Approximately 20 percent of fraud cases, approximately 16.9 percent of hacking and illegal access, and approximately 9.1 percent of viruses, worms, spyware and logic bomb could be classified into the category of medium security.

Only 17.4 percent of attack and sabotage, approximately 12.5 percent of miscellaneous (including embezzlement and corruption), and approximately 8.5 percent of hacking and illegal access succeeded in penetrating a well-protected computer system.

4.8. Complexity of Cybercrime

All the cases of data theft and espionage seem uncomplicated to commit. Approximately 87.5 percent of miscellaneous cases (including embezzlement and corruption), 80 percent of fraud cases, 73.9 percent of attack and sabotage cases, 66.7 percent of ID theft cases, and 66.1 percent of hacking and illegal access cases involved no complicated techniques or techniques that could be available to the most common computer or network user at the time of committing such offences.

Approximately 27.3 percent of viruses, worms, spyware and logic bomb cases, 20 percent of fraud cases, 12.3 percent of hacking and illegal access cases, and 8.7 percent of attack and sabotage cases are committed with moderately sophisticated techniques.

Cases of viruses, worms, spyware and logic bombs might involve the most complicated techniques, 72.7 percent of which fell into the most complicated category. Approximately 33.3 percent of ID theft cases, 18.3 percent of hacking and illegal access cases, 17.4 percent of attack and sabotage cases, and 12.5 percent of miscellaneous cases might involve complicated techniques or techniques unavailable to common users at the time of committing such offences.

4.9. Imprisonment Sentences

The punishments for many cases are labelled as "to be decided." This study calculated the punishment of the sentenced cases. The average imprisonment sentence for the data theft and espionage cases is 50 months, which is the longest among all the categories of cybercrimes. Cases of virus, worms, spyware, and logic bomb; and miscellaneous offences have the same average imprisonment sentence of 40.3 months. Fraudsters received an average imprisonment sentence of 32.5 months. Attack and sabotage cases are sentenced to an average imprisonment term of 28.1 months. The shortest average imprisonment term, 21.9 months, is imposed on hacking and illegal access perpetrators, namely the hackers.

The total imprisonment term imposed on the reported 53 offenders is 1429 months, with an average of shorter than 27 months. Among these cases, the longest imprisonment is 96 months, while the shortest is only one month.

4.10. Fine Sentences

A fine is typically imposed on perpetrators of hacking and illegal access, and attack and sabotage cases. Overall, exactly ten cases ended with a fine of less than USA\$10,000, nineteen cases with a fine between USA\$10,000 and USA\$100,000, twelve cases with a fine between USA\$100,000 and USA\$1 million, and two cases with a fine over USA\$1 million (one case was fined USA\$2 million and the other case was fined USA\$7.8 million).

The fine imposed on 43 offenders totalled USA\$13.45 million, with an

average of USA\$312,780. However, this sum is largely due to the heavy fines in two cases where the offenders were fined USA\$2 million and USA\$7.8 million, which contributed to an excess of USA\$228,000 for the calculation of average fine. If these two cases are excluded from calculations, the average fine is approximately USA\$89,000.

*

5. DISCUSSION AND CONCLUSION

THE SUBJECTS OF CYBERCRIMES CAN BE either insiders or outsiders. Many studies have found that insiders constitute a great threat to employers' systems. However, younger juveniles are less likely to be employed and may represent the increasing number of outsiders engaged in cybercrimes. On the other hand, the nature of cybercrime is such that there is no age limit. Anyone who can use computers and the internet can commit a cybercrime.

In my opinion, the concept of white-collar crime cannot fit the situation of cybercrime. Although white-collar crime emphasizes the employment and social status of the criminals, I consider that one of the most relevant factors in white-collar crime is the knowledge criminals have acquired from both their pre-employment education and their occupational career. It is not oversimplified to view white-collar crime as a knowledge-based offence, compared with violence-based traditional offences. As opposed to these two conceptions, cybercrime could be either knowledge-based white-collar crime or knowledge-based cyber violence. Overall, there is a reluctant distinction between cybercrime, white-collar crime and even violent crime.

However, it is reasonable to conclude that when there were few computers, employees in the computer-related industries were among the small number of computer users. They had more chances to commit an offence against their employers. With the prevalence of personal computers and the development of the internet, insiders maintain the advantage of having better knowledge about access control mechanisms, assets management systems, and overall loopholes. Insider knowledge, convenience, and directness encourage employees to commit cybercrimes. As the United States Secret Service and CERT Coordinator Center's study disclosed, minimal technical skill was required to launch cyberattacks on the banking and finance sector.³⁴

In addition, insiders are exposed to the negative psychological influence derived from their information work environment. Shaw, Ruby and Post identified characteristics that increase the tendency towards illegitimate and harmful behaviour of the employees: "computer dependency, a history of personal and social frustrations (especially anger toward authority), ethical flexibility, a mixed sense of loyalty, entitlement, and a lack of empathy."³⁵

On the other hand, the offences by insiders involve a less complicated

34. Marisa Reddy Randazzo, Michelle Keeney, Eileen Kowalski, Dawn Cappelli, and Andrew Moore, "Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector," Technical Report, CMU/SEI-2004-TR-021 (Carnegie Mellon Software Engineering Institute, 2005), <<http://www.sei.cmu.edu/pub/documents/04.reports/pdf/04tr021.pdf>> at pp. 9, 23. Insider was defined as "current or former employees or contractors." *ibid* at p. 5.

35. Shaw, Ruby, and Post, "The Insider Threat" *supra* note 23 at "Personal and Cultural Vulnerabilities."

process of being traced, detected and investigated than those by outsiders. If we could not judge whether insiders or outsiders are liable for more cybercrimes, we should firstly consider the question of who is more likely to commit cybercrimes and who is more likely to be caught. The insiders are both more likely to offend and more likely to get caught than outsiders. Furthermore, it is more efficient for law enforcement to uncover an inside than an outside attack. They are rationally more likely to pay more attention to the current and previous employees. The outside incidents or international disturbances would possibly be disregarded at the first sight of the investigation, unless it arouses broad concern in international society.

In summary, the study found that males are responsible for a majority of cybercrime. The cybercriminals are primarily between the ages of 17 to 45 years old. Domestic perpetrators constitute the absolute majority of the cybercriminals. Outsiders are four times more likely to be involved in cybercrimes than insiders. A large part of cybercrimes did not cause economic loss. However, once economic losses were involved, the average sum could reach as high as USA\$1 million. The most vulnerable interests are in the private sector, even though threats to the public sector have usually been given more attention. The security levels of the victims are surprisingly weak, vulnerable to unsophisticated cybercrimes. Penalties against cybercrime, whether imprisonment or fines, are generally light.

The limit of this study is that the sample cases are randomly selected and published on the United States of America Department of Justice website. They could be regarded as typical cybercrime cases, but it is difficult to say whether they could be considered representative of cybercrimes happening in the United States. Therefore, this study is an explanation of the cases as examined. The sample survey method is usually used to give a sketch of the whole through the part, but this study warns against generalization of its findings to all cybercrimes. To avoid the shortcomings in the methods, the ideal study should cover a random sample in a wider range of cases, if it is available.

Appendix: Table of Statistical Data

115 cases 151 persons 1 company		Hacking, illegal access		Attack, sabotage, botnet		Virus, worms, spyware, logic bomb		Data theft, espionage		ID theft		Fraud		Other: embezzling, corruption		
Gender	No.	No.	%	No.	%	No.	%	No.	%	No.	%	No.	%	No.	%	
Male	61	96.8		23	100	11	100	7	100	26	100	7	100	13	92.9	
Female	2	3.2		0	0	0	0	0	0	0	0	0	0	1	7.1	
Total	63	100		23	100	11	100	7	100	26	100	7	100	14	100	
Age																
-16	2	3.2		0	0	1	0	0	0	0	0	0	0	0	0	
17-25	20	31.7		7	30.4	2	18.2	0	0	5	19.2	3	42.9	4	28.6	
26-35	18	28.6		6	26.1	2	18.2	3	42.9	1	3.8	2	28.6	7	50	
36-45	12	19		2	8.7	3	27.3	1	14.3	0	0	2	28.6	1	7.1	
46-	1	1.6		1	4	1	9.1	2	28.6	1	3.8	0	0	0	0	
N/A	10	15.9		7	30.4	2	18.2	1	14.3	19	73.1	0	0	2	14.3	
Perpetrator																
Insider	15	23.8		3	13	2	18.2	7	100	0	0	4	57.1	1	71	
Outerider	48	76.2		20	87	9	81.8	0	0	26	100	3	42.9	13	92.9	
Former employee	Inclu. 8	12.7		Inclu. 10	43.5	0	0	0	0	0	0	0	0	1	7.2	
Loss	No	No		N/A	N/A	7	N/A	5	N/A	1	N/A	4	N/A	6	N/A	
-10k	33	4(21k)		N/A	2(10k)	N/A	1(5k)	N/A	N/A	0	N/A	0	N/A	0	N/A	
10k-100k		15(753k)		N/A	3(69k)	N/A	0	N/A	N/A	0	N/A	0	N/A	0	N/A	
100k-1m		4(1076k)		N/A	6(1.679M)	N/A	0	N/A	N/A	0	N/A	1(384k)	N/A	1(875k)	N/A	
1m+		5(34.3M)		N/A	0	N/A	3(93M)	N/A	0	N/A	2(8M)	N/A	0	N/A	1(6.3M)	N/A
Total	28(36.15M)	N/A		11(1.758M)	N/A		4(93.005M)	N/A	1(5k)	N/A	2(8M)	N/A	1(384k)	N/A	27(175k)	N/A

		115 cases		151 persons		Hacking, illegal access		Attack, sabotage, botnet		Virus, worms, spyware, logic bomb		Data theft, espionage		ID theft		Fraud		Other: embezzling, corruption	
		No.	%	No.	%	No.	%	No.	%	No.	%	No.	%	No.	%	No.	%	No.	%
Citizenship	Foreigner	1 case	N/A	1 case	N/A	0	N/A	0	N/A	1 case	N/A	1 case	N/A	1 case	N/A	1 case	N/A	1 case	N/A
Imprisonment	1-6	5(24)	N/A	2(11)	N/A	0	N/A	0	N/A	0	N/A	0	N/A	0	N/A	0	N/A	0	N/A
	7-12	9(10)	N/A	0	N/A	0	N/A	0	N/A	0	N/A	0	N/A	0	N/A	0	N/A	0	N/A
	13-24	7(13)	N/A	4(8)	N/A	2(8)	N/A	1(18)	N/A	0	N/A	0	N/A	0	N/A	0	N/A	0	N/A
	25-36	7(22)	N/A	2(7)	N/A	0	N/A	1(36)	N/A	0	N/A	0	N/A	2(65)	N/A	2(70)	N/A	2(70)	N/A
	>37	4(21)	N/A	2(11)	N/A	1(41)	N/A	1(96)	N/A	0	N/A	0	N/A	0	N/A	1(51)	N/A	1(51)	N/A
TBD		27	N/A	13	N/A	5	N/A	3	N/A	3	N/A	3	N/A	3	N/A	5	N/A	5	N/A
Fine	<10k	7(31.6)	N/A	1(5k)	N/A	1(5k)	N/A	0	N/A	0	N/A	0	N/A	0	N/A	0	N/A	1(5k)	N/A
	10-100k	13(512.6)	N/A	5(18.8k)	N/A	1(17k)	N/A	0	N/A	0	N/A	0	N/A	0	N/A	0	N/A	0	N/A
	100k-1m	50(1.368m)	N/A	4(63.8k)	N/A	0	N/A	0	N/A	0	N/A	0	N/A	2(624k)	N/A	1(250k)	N/A	1(250k)	N/A
	>1m	0	N/A	0	N/A	1(2m)	N/A	0	N/A	0	N/A	0	N/A	0	N/A	1(7.8m)	N/A	1(7.8m)	N/A
TBD		32	N/A	13	N/A	7	N/A	6	N/A	3	N/A	3	N/A	3	N/A	5	N/A	5	N/A
Nature of victim	Public	8	13.6	4	18.2	0	0	0	0	0	0	0	0	0	0	0	1	12.5	
	Private	41	69.5	17	77.3	9	81.8	5	100	3	100	4	100	4	100	7	87.5		
	Private, public	9	15.3	0	0	1	9.1	0	0	0	0	0	0	0	0	0	0	0	
	Public health and safety	1	1.7	1	4.5	1	9.1	0	0	0	0	0	0	0	0	0	0	0	

115 cases 151 persons 1 company			Hacking, illegal access	Attack, sabotage, botnet	Virus, worms, spyware, logic bomb	Data theft, espionage	ID theft	Fraud	Other: embezzling, corruption	
Security	No.	%	No.	%	No.	%	No.	%	No.	%
Strong	5	8.5	4	17.4	0	0	0	0	0	12.5
Medium	10	16.9	0	0	1	9.1	0	0	1	0
Weak	44	74.6	19	82.6	10	90.9	6	100	3	87.5
Technique	Complicated	11	18.6	4	17.4	8	72.7	0	1	33.3
availability to others	Medium	9	12.3	2	8.7	3	27.3	0	0	0
Simple	39	66.1	17	73.9	0	0	6	100	2	66.7
others									4	80
									7	87.5

Home	Table of Contents	Titles & Subject Index	Authors Index
----------------------	-----------------------------------	--	-------------------------------

E-marketing, Unsolicited Commercial E-mail, and Legal Solutions

[Xingan Li](#)

Faculty of Law, University of Lapland, PL 122, 96101 Rovaniemi, Finland. E-mail: xingan.li (at) yahoo.com

Received February 18, 2006; Accepted March 30, 2006

Abstract

The purpose of this paper is to explore the legal solutions to unsolicited commercial e-mail. The advantages of e-mail enable it to be one of the most important e-marketing instruments. Spammers are also motivated by potential profits in spamming. The low costs and high benefits of the spammers, and the high costs and low benefits of the spammed determine the illegal nature of the spamming. The spam poses challenges for e-mail recipients' property rights, fair trade, public morals, cybersecurity, personal data protection, and involves other concerns as well. In dealing with spam, technical and marketing solutions cannot work alone without the legal mechanisms. The legal regulation is justified by balancing the interest between senders, service providers and even users. Criminal sanctions, civil remedies, and international harmonization are alternative steps in establishing legal solutions. As a necessary part of the legislation, punishment for unsolicited commercial e-mails should be more severe. Still, there are a number of limitations to the effectiveness of law enforcement against spamming. Spam must be eliminated by comprehensive mechanisms.

Keywords

Direct Marketing, Spam, Unsolicited Commercial E-mail, Legal Solutions

Introduction

With the development of e-commerce and the prevalence of the Internet, e-mail has become the primary means of communications and marketing. Compared with the traditional marketing tools, e-mail has obvious advantages. However, the abuse of e-mail disturbs the normal communications services, and influences the environment for the public to use the Internet. The reception of unsolicited electronic messages and commercial information become a pervasive social and economic problem. The difficulties in identifying the senders and in compensating the recipients' losses further prove the uncontrollability of the Internet. Spamming impedes the effective application of telecommunications to the individual and business communication, baffles the consumers' acceptance of legal e-marketing, and in turn, hinders the growth of the e-commerce. Many individuals and institutions are making efforts to seek solutions to the problem (for example, [Coalition Against Unsolicited Commercial Email](#), 1999; [Cobb](#), 2003; [Direct Marketing Association](#); [Federal Trade Commission](#), 1998, 2003; [Ferguson & Piragoff](#), 1997; [Gartner Consulting](#), 1999; [Gauthronet &](#)

[Drouard](#), 2001; [Goodman & Rounthwaite](#), 2004; [Hansell](#), 2003; [International Telecommunication Union](#), 2004; [Khong](#), 2001, 2004; [Midnet Media](#), 2003; [Mail Abuse Prevention System](#), 2004; [Organization of Economic Cooperation and Development](#), 2003, 2004; [Peppers & Rogers](#), 2000; [World Summit of Information Society](#), 2003 and many others). In order to ensure the convenience of the Internet use and improve the security and efficiency of the Internet environment, some countries have implemented specific legislation to regulate spam; the European directives required the member states to incorporate commercial e-mail rules in the provisions on privacy and telecommunications. Organization of Economic Cooperation and Development ([OECD](#)) called for legislation and international cooperation in combating spam. Based on documentary analysis and empirical study, this paper explores the threats of the unsolicited commercial e-mail and the difficulties in dealing with the problem, analyzes the dilemmas in combating spam under the present legal framework, and suggests possible countermeasures.

Background and definition of spam

As the capability of computers and networks to process information increases, "a wealth of information" can lead to a "poverty of attention" ([Simon](#), 1982). Unsolicited business e-mail (UBE) or unsolicited commercial e-mail (UCE) represents an example that e-mail users have to deal with the superfluous information they do not expect to consume. It is generally called bulk mail or spam. It turns out that spam has evolved into a large amount of information garbage, polluting the environment of e-marketing. When we talk about the phenomenon of spam, we are talking about a negative externality in e-marketing that people try to get rid of. It brings about the negative image of e-marketing, frightening e-mail users from trusting the e-mail communications.

Up to April 2005, the population of global e-mail users increased to 683 million, with almost 1.2 billion lively accounts. The e-mail marketing has been regarded as one of the most successful marketing means on the Internet ([Niall](#), 2000). Unfortunately, with the increase of the e-mail usage, two thirds of the total 130 billion messages sent and received everyday are unsolicited ([Radical Group](#), 2005).

In nature, e-mails can be a kind of information goods, for example, messages provided by the paid subscription services; while at the same time, e-mail can also be a kind of bads, in case the subscribed paid information are harmful to general public or to specific groups or a certain person. If the information is provided free of charge, it becomes an externality. When the messages are useful, they are positive externalities; when they are harmful, they become negative externalities. Whether they are with charge or without charge is decided by the sender; but whether they are useful or harmful, is decided by the recipient.

Nonetheless, spam sent out to multiple recipients, blemishes the name of e-mail marketing ([Wreden](#), 1999; [Wright and Bolting](#), 2001). Institute of Management Technology ([IMT](#)) Strategies (2001) found that the e-mails that the users never read are increasing, and the consumers tend to constraint or interrupt the e-commercial contacts. Before the universal access to the Internet was available, the e-mail spam was really a small trouble. But today, most users worldwide are confronted with this problem nearly everyday. The problem has increasingly important influence on the consuming behaviors. In an [InfoWorld](#) article (2003), a survey disclosed that over forty percent of respondents answered unsolicited e-mail as the worst problem in the field of information technology industry in the previous year. The scale and effect of the spam prevalence implies that spam has become "significant and growing problem for users, networks and the Internet as a whole" ([World Summit on the Information](#)

[Society](#) (WSIS) Declaration, 2003, paragraph 37).

Most people have some unclear awareness that spam at first came from the "spam skit by Monty Python's Flying Circus"¹ ([Templeton](#), 2003). However, according to [Templeton](#) (2003), the history of spam can be traced back to the late 1970's with a number of network services that were sent multiple mailings, these initial group mailings were not considered annoying and as a result they got the chance of wide online spread ([Templeton](#), 2003). [Kelly](#) (2002) explored the history of spam and believed that it was born on April 12, 1994. We can also reasonably judge that it was until the Internet was in its wide usage, when unsolicited e-mail posed a real threat.

The consensus on the definition of unsolicited e-mail is nearly reached among academia, legislature, and law enforcement, even though the actual legal practices are few. [Mail Abuse Prevention System](#) (2004) defined spam as:

"An electronic message is 'spam' if: (1) the recipient's personal identity and context are irrelevant because the message is equally applicable to many other potential recipients; and (2) the recipient has not verifiably granted deliberate, explicit, and still-revocable permission for it to be sent; and (3) the transmission and reception of the message appears to the recipient to give a disproportionate benefit to the sender."

Although the definition of e-mail spam only denotes to the sender and recipient, they can be understood as covering individuals, organizations, enterprises, and public institutions. It is a common concern in local, national, and international layers. During the Geneva phase of the World Summit on the Information Society, spam was identified as a potential threat to the full utilization of the Internet and e-mail ([International Telecommunication Union](#), 2004).

Classification of spam is vital from a legal standpoint, because most spam legislation targets a particular type, such as business e-mails, or deceptive spam. The United States Federal Trade Commission identified twelve most likely spam scams: business opportunity scams, making money by sending bulk e-mailing, chain letters, work-at-home schemes, health and diet scams, easy money, get something for free, investment opportunities, cable descrambler kits, guaranteed loans or credits on easy terms, credit repair scams, and vacation prize promotions ([Federal Trade Commission](#), 1998).

The unsolicited e-mail being a central concern, spam can also come from other sources, such as newsgroups, mobile phones Short Message Service (SMS) and instant messenger services. The legal solution to these kinds of spam is possibly in common, and countries have laws to cover spam of these and other forms of media, but this paper is mainly concentrated on e-mail spam.

Comparison between traditional and e-mail advertisements

Besides interpersonal interaction through e-mail, e-mail has also broad usage in advertising as well. What accompanies the unsolicited commercial e-mail is that it parallels with the legal advertisements, that is, e-mail advertisements. To better understand the phenomenon of spam and find effective preventive mechanisms, the following section contributes to compare the advantages and disadvantages of traditional advertisements, particularly postal advertisements, and the e-mail advertisements (See Table 1).

Table 1: Comparison between traditional advertisements and e-mail advertisements

Compared Items	Traditional advertisements	E-mail advertisements
Public consciousness	Familiar	Unfamiliar
Scope	Indirectly attention-getting	Direct attention-getting
Basis of trust	Publicity	Confidentiality
Targeted audience	Mainly subscriber	Mainly non-subscriber
Censorship	Involving intermediary censorship	Lacking intermediary censorship
Costs	High	Low
Form of trade	Traditional form to traditional form	Electronic form to traditional form or electronic form
Sending and reply addresses	Provided, mostly the same	Provided or not, same or different
Receiving addresses	Limited territorial range. The wider the territorial range, the higher the costs	Unlimited territorial range. Costs independent of territorial range.
Jurisdiction on disputes	Easy to ascertain according to existing laws, regulations and cases.	Difficult to ascertain. Lacking ready laws, regulations and cases.
Regulation on spam	Yes	No
Possibility of regulation on spam	Easy	Difficult
Collection of evidence on spam	Converse investigation: from consumer to registered or licensed intermediary and advertiser.	Difficult to investigate. No such registration or license.
Deterrence of punishment on spam	Strong	Weak
Possibility of recommitment of spamming	Low	High
Effect of spam	As the increase of traditional advertisements, advertisers and intermediaries better off, while recipients better off, or no change.	As the increase of unsolicited e-mail advertisements, advertisers and intermediaries better off, while recipients will worse off.

The e-mail marketing has the following advantages:

- (i) Being directly attention-getting. In most cases, the e-mail advertisements are similar to traditional advertisements in the form that the audience are not strictly divided and designated, such as the advertisements in newspapers, magazines, radios, TV programs, outdoor advertisements, or even online banner advertisement. But the e-mail marketing has the high potential to provide personalized information according to the users' different needs, hobbies, and interests. It is not strange that a professor receives advertisements on conferences, sales of books, and so on; that a professor of economics receives more specified information on conferences on economics, sales of economic books, and so forth. Many other forms of advertisements do not have so

concentrated an audience. [Peppers and Rogers](#)' study (2000, p 4) discovered that the one of the success factors enabling the e-mail marketing to work well is "high response rates." The average reply rate of e-mail is 5-15 percent versus 1-2 percent for direct mail and 0.005-1 percent for banner advertising, while the e-mail marketing creates a positive effect on branding efforts ([Midnet Media](#), 2003, p.1).

- (ii) Interactive marketing. The e-mail marketing can keep more customers. The decrease of costs and timelines permits business to communicate with customers more frequently. Regular e-mail marketing to existing customers generates a 15-50 percent increase in overall online trade. Engaging customers in a two-way dialogue enhances customer satisfaction and yield quicker response (C.f. [Sandiego Media](#) Inc., 2005).
- (iii) Confidentiality. The contents of e-mail advertisements are not necessarily confidential. E-mail is not in itself the most confidential form of communications. But for a certain users in a certain environment, the e-mail marketing is like a consult or negotiation in a closed room. What the user decide to buy, to whom the user pays, and what and from which address the user receives, are not directly showed to anyone else. In case that the user consumes digital information, the e-mail and other electronic or online marketing might be the most suitable means.
- (iv) Low cost. The e-mail marketing lowers costs and increases profits. The e-mail marketing supplies cost-saving benefits, such as no printing, mailing or media expenditure; allows for more frequent customer conduct, which turns into higher income; average costs of 0.03 to 0.1 dollars for each e-mail, versus 2 dollars for direct post and up to 3 dollars for telemarketing; customer acquisition costs average no more than 24 dollars for e-mail versus 82 dollars for public relation, 958 dollars for print advertisements, and 1,457 dollars for radio advertisements ([Midnet Media](#), 2003, p.1).
- (v) Diversified forms of trade. The e-mail marketing serves both traditional and digitalized goods. The goods are usually exhibited online. For traditional goods, though the electronic exhibition is not as intuitionistic as show window, or door-to-door marketing, the multimedia explanation may provide more comprehensive a presentation than any other forms of marketing. In case of digital goods, the e-mail marketing has the unique advantage in providing sample texts, and audio or video clips. In fact, many online book stores, music and video dealers, and software vendors all provide some kinds of sample to show their goods. The e-mail marketing can directly link to these online markets and goods.
- (vi) Location independent. The senders and the recipient of e-mails are both location independent. The senders can send e-mails from anywhere of the world to recipients located anywhere in the globe (if they are not outside the earth). Trans-border marketing is not limited by the national boundary. A nearly uncontrollable route realizes the flow of goods, particularly digital goods. Even if it is traditional goods, the uncontrollable information might also cause the traditional control of trans-national flow of goods more burdensome. All in all, the trans-territorial flow of goods can benefit greatly from e-mail marketing.
- (vii) Advertisers better off; and intermediaries might also better off. As a natural effect, with the increase of e-mail marketing, the advertisers will surely better off. The voluntary intermediaries will also better off, because a portion of the profits is transferred from the advertisers to the intermediaries.

The disadvantages of e-mail advertisement are:

- (i) Most people are less familiar with e-marketing than traditional advertisements. Less people are more familiar with e-mail marketing than

traditional advertising. But more and more people are more familiar with the new advertisements than ever.

- (ii) Targeting both subscriber and non-subscriber. This may induce more consumers, but may also annoy e-mail users. In fact, different forms of traditional advertisements are designed to different audience. Some forms do not distinguish subscriber or non-subscriber, such as radio, TV and outdoor advertising. But traditional postal marketing mainly targets subscribers, together with newspaper and magazine advertising. With e-mail advertisements, the businesses can limit marketing to subscribers, but can also extend to non-subscribers in order to get more profits. This advantage for senders becomes the greatest disadvantage for recipients.
- (iii) Lacking intermediary censorship. Unlike traditional advertisements that have been published on media that are managed by intermediaries, the e-mail marketing is actually direct marketing- more direct in the sense of business-to-consumer, but at the same time more indirect in the sense of no longer face-to-face. The necessary censorship on the process of information provision is missing. Subsequently, the transaction process is also less monitorable and less controllable.
- (iv) Sender's genuine identity and displayed information might be different. The falsification of sender's identity and address might mislead the consumer to open the unsolicited e-mail. The reply address might be invalid when the recipient replies to refuse further messages. The recipients have less choice in deciding whether or not to receive this kind of e-mail.
- (v) Lack of dispute solution mechanism. The possibility of regulation on e-mail marketing is law. The jurisdiction over disputes is difficult to determine. The laws, regulations, and rules, particularly international harmonization are not ready. In addition, collection of evidences is confronted with great obstacles.
- (vi) Weak deterrence of punishment on abuse of e-mail marketing. The spammers have high possibility of recommitment, motivated by monetary interests. As a result, the recipient might worse off due to absence of self-determination, while the intermediaries might also worse off due to the absence of profit transfer agreement.

The advantages and disadvantages seem more and more beneficial to the senders but less and less beneficial to the recipients. As a result, the senders have the stronger incentive to send more marketing e-mails, while the recipients have the stronger to receive less. The overuse of e-mail marketing by the businesses will lead to underuse by the consumers.

Challenges of spam to the society

The advantages of e-mail marketing greatly upgrade the utility of e-mail in business. Both the legal and illegal commerce discover this efficient instrument in harvesting money from the market. The following summarizes a list of common challenges of legal sense that the spam brings to the society.

The first challenge is against e-mail recipients' property rights. The spammer infringes the property rights through two ways. On the one hand, spammers usually transfer the cost of sending bulk e-mails to others, including individuals, e-mail service providers (ESPs) or Internet service providers (ISPs), for example, intrusion others' computers or servers to send e-mails, or evasion the reasonable fees payable to the service providers. On the other hand, spammers usually practice fraud and deception in spamming. Spammers disguise the origin of their messages so as to ensure that the users read their messages. [Federal Trade Commission](#) (2003) reported that 66 percent of spam messages are fraudulent in the "from" or "subject" lines, or in the message

itself. For example, if the subject line includes the term such as "reply", "your required information", "your free laptop", "free travel chances", etc, it is highly possibly that the users will open the e-mail and find if these are valuable messages. As for the contents, many unsolicited e-mails offer various deceptive or misleading representations. The most common fraud schemes include the Nigerian scam, online chances of making money, and drugs sales, etc. In a successful detected case, the FBI in the United States and the Spanish police arrested 310 people who were the Nigerian conspirators of a bogus lottery scam involving 100 million Euros. The scam victimized more than 20,000 people in 45 countries ([Libbenga, 2005](#)).

The second challenge is targeted at fair trade. Contents of most unsolicited e-mails involve false advertisements or situation leading to misunderstanding. Due to the facility of transfer, such e-mails incorrectly relay erroneous information, and mislead the recipients and consumers in the bargaining. Besides the breach of the regulations on consumer protection and constitution of criminal fraud, the false advertisements might distort the normal market of goods and services, harm the normal trade order, and reduce the consumers' confidence ([Taiwan Ministry of Transportation and Communications, pp. 6-7](#)).

The third challenge is offending public morals. Unsolicited e-mails are usually not targeting specific e-mail users, among which children are highly possibly to be harassed. Because the spam messages often contain contents inappropriate for children, such as the hyperlinks of pornographic websites, pornographic pictures, and adult entertainment products and services, the pornographic spam has become a public risk for the growth of the children. From the pornography industry revenue statistics, it is apparent that the Internet-related revenue has already reached a noteworthy scale. What is worse is that the average age of first Internet exposure to pornography is as low as 11 years old, and 90 percent of the children between 8-16 years old have viewed pornography online ([TopTenReview, 2005](#)).

A relevant problem is that in some East Asian and Middle East countries, creating, copying, selling, and spreading pornography might lead to arrest and conviction (See example, Penal Law of China 1997, Articles 363-367). In addition, merely possession, and browse of pornography is traditionally prohibited. The unsolicited e-mails make it difficult to judge whether the existing punishments are applicable to e-mail users who passively receive and "keep" e-mails with pornographic contents. For example, Management Regulations on Internet Online Service Business Location provides that the manager of Internet online service business location and the Internet users must not create, download, copy, view, release, spread or use by other means the information containing obscenity contents (China State Council Management Regulations on Internet Online Service Business Location 2002, Article 14).

The fourth challenge is a threat to cybersecurity. The security problems brought about by the spam generally require the interaction between the users and the messages. The large volume of spam, the malicious programs and malicious linkages contained in the messages are the main threats ([PC World, 2003](#)). In recent years, many of the most harmful malicious programs have been spread through exploiting e-mails.

The fifth challenge involves personal data protection. There is little exception in the available literature and legislation on spam that does not emphasize the identity theft. Many spammers send their messages by unauthorized use of other individuals or organizations' accounts ([OECD, 2004](#)). The e-mail addresses harvesting software can collect this information automatically from the webpages ([Boldt, Carlsson and Jacobsson, 2004, p. 8](#)). Therefore, the misuse of spamware and the collection and use of e-mail addresses are among the focuses of the legal regulation. If the e-mail

address includes enough information to identify the user, the collection and use of such an e-mail address should under the consent of the user. Without such consent, the collection and use of the address in the spamming invalidate the privacy protection.

The sixth challenge is comprehensive. Besides the above aspects, spam is also involve in other content-related and goods-related transgresses and offences. The examples of the former category are online piracy of intellectual property, spreading of malicious programs and codes, defamation, slander, and libel, and so on. The examples of the latter category are sales of controlled goods, such as drugs, prescribed medicine, and weapons; providing services, such as auction, financing, tourism, dating, prostitution, gaming, gambling, raffling, bonus, and lottery.

In sum, at least at present, the ease of using spam to offer goods and services increases the volume of spam. Sophos statistics showed that global spam at the end of 2004 has reached 3 trillion messages, with an estimated cost of 131 billion dollars ([EquiP Technology and Cipher Trust](#), 2004). In addition, according to an Industrial Development Corporation (IDC) study, worldwide revenue for anti-spam solutions will exceed 1.7 billion dollars in 2008 ([IDC](#), 2005).

Costs and benefits of the spammer and the spammed

1. The costs and benefits of the sender

Whether the spammer send the spam is thought by economists as controlled by "the invisible hand"² of interests. According to [Khong](#) (2004), although it is difficult to measure the costs and benefits of the spammer, if the benefit obtained from the activity outweighs the cost, then the spammer will undertake the spamming activity. It follows that if there is one successful commercial transaction, the spammer can realize his/her benefit. The costs that are involved in the spamming can be roughly estimated in the following aspects:

First, bandwidth cost. It is inevitably to involve the cost of bandwidth in the message sending. According to [Living Internet](#) (2005), as a form of communication across global distances, e-mail is relatively the cheaper way. Based on a very conservative cost of 10 dollars a gigabyte for bandwidth, Living Internet showed that every 50 thousand e-mails cost one dollar in bandwidth costs. That is to say, the per message bandwidth cost is only 0.000020 dollars. If the spammers undertake these costs, the monetary investment will be very tiny compared with the possible income from the spamming.

Second, costs in sending message. Besides bandwidth costs, there are also other costs associated with sending a message. This is usually measured by how much the spammer is willing to do the spamming. According to [Goodman and Rounthwaite](#) (2004), the higher price is about 0.001 dollars per message, the lower price is about 0.000025 dollars per message. The cheaper charges range from 0.0001 to 0.0003 dollars per message.

Third, to obtain users' e-mail address may also involve some kinds of costs. But the actual cost may depend on the ways in which the addresses are harvested. According to Sadowsky, the spammer can obtain users' e-mail address in the 13 situations ([Sadowsky et al.](#), 2003, p. 55). But obviously, the most convenient and least expensive way is to harvest e-mail addresses automatically with specific software. The software are also available from Internet, either free of charge or with an inexpensive price.

Even trickier, the revenue of spammer from sending message has been found high in a few studies. [Goodman and Rounthwaite](#) (2004) cited the following information in clarifying how much per message revenue would be. They cited that [Grimes](#) (2003) had reported one person had had the revenue of as much as 0.0005 dollars per message, but was willing to do as little as 1,000 dollars per mailing; as little as 0.0000125 dollars per message. Other information they cited was from a *Wall Street Journal* article, reporting that a person obtained 360 dollars or sending 10 million messages, around 0.000036 dollars per message ([Moran](#), 2002).

The above information indicates that the costs of the spammer are increasingly low, while the revenue is increasingly high. [Hansell](#) (2003) found that compared to the cost of 190,000 dollars for one million conventional bulk-rate postal mails, the marginal cost of sending a marketing message to one million recipients by electronic mail is less than 2,000 dollars. He estimated that commercial e-mail is profitable if one recipient in 100,000 makes a purchase. The fact that the spam can be sent at very low cost and in a great quantity has attracted direct marketing companies to use spam e-mails for advertisement. [Cobb](#) (2003, p.2) suggested the concept of "the parasitic economics of spam," meaning that the act of sending a message costs the sender less than it costs all other parties impacted by the sending of the message. In reality, some spammers pay nothing for sending their messages, hijacking resources that belong to others.

2. The costs and benefits of the spammed

The costs induced by the spam to the spammed have a wide coverage. They include the waste of the users' time, bandwidth and storage, cost of anti-spam solution, and cost of overloading at the mailbox.

First, the topic of whether the waste of time in dealing with the spam is disputable. Spam messages are annoying in that the users have to spend time and money dealing with them. In daily life, some people argue that they know e-mail well and it is easy to identify spam messages from useful e-mails. Even if there are some bulk mails, the user needs only a few seconds to browse the address, subject, content, signature, etc in making a judgment. To delete them is also not so complicated. They doubt how the problem can be so serious and so wasteful. In fact, meeting with messages well falsified in address and subject lines, the user is impossible to judgment whether this is a spam or a message from a contact. When the message is open, the user has to browse the contents and signature to make the final decision. If the message begins with information of his interests, the users have to spend yet more time to decide whether or not to delete the message. The average time and money lost in processing a single message might not be so significant. But the aggregate loss of time and money in aggregate taken in dealing with these messages might be huge.

The time the users spend on dealing with spam messages can be quantified in a way of counting numbers of messages the users receive everyday, and the time spent on making judgment on whether the messages are spam and deleting them. In some services companies, the treatment of these messages needs special care so as not to ignore the customers' requests, complaints, and business communications. [EquiP Technology and Cipher Trust](#) (2004, p.1) found that the average e-mail user receives up to 70 e-mails a day. According to [Zeller](#) (2005), a December 2004 survey suggested that Internet users spend an average of 10 working days per year dealing with spam, and at least some industry analysts estimated that the yearly cost of spam to business due to lost productivity and additional network maintenance costs will be around 50 billion dollars.

Second, spam also induces costs of the bandwidth and storage. [Khong](#) (2001) pointed

out that in addition to the losses of the users, the spam also has great impact on e-mail service providers (ESPs). The European Union estimated the global bandwidth costs of spam at 8-10 billion dollars annually ([EquiP Technology and Cipher Trust](#), 2004, p. 2). The potential threats might even severe to cause an ESP's network to shut down ([Goodman](#), 2000). The interruption of services is unfortunate for both the providers and users in causing business, confidence, and other losses.

Third, the influx of spam has caused many people and organizations to deploy some form of anti-spam solution. A European Commission study estimated that the costs associated with these solutions might come up to 10 billion euros per year worldwide ([Gauthronet & Drouard](#), 2001). [Gartner Consulting](#) (1999, p. 4) found that the longer an e-mail user kept an e-mail account, the more likely he would be spammed. It indicates that spam is a more severe threat to the established users than the new comers, and a more severe threat to the users more dependent than the users less dependent on e-mail. That is to say, the more possible the users benefit from the e-mails, the more possible they bear losses from spam. The increased profits of the spammer are just based on the increased loss of the spammed. It is reasonable to deduce that the spamming business would growth in pace with the development of the e-commerce.

Finally, another side effect of the spam is that it corrupts e-mail services, fills up users' mailbox with useless information, and decreases the usefulness of the e-mail service. Even worse, if the e-mail address has ever been put on the institution's website, or personal homepage, it is highly possibly that the address will be harvested, sold, and abused by spammers. Under these circumstances, the number of spam messages might increase in an unexpected pace. I keep an e-mail address provided by a high profile website. It has been put to the Internet for a few occasions. Recently, the average number of spam messages per day may reach one hundred. Although the fortunate bulk mail prevention function by the provider works well, and most bulk mails are automatically put into the specific folder, sometimes, it is inevitable that useful messages are also identified as spam, and the inbox is still filled with dozens of spam messages everyday. Most of the spam messages can really be judged through the subject or address lines. To delete them needs a few seconds everyday. The most annoying is that it is really difficult to look for the useful messages from dozens of useless messages received unexpected. The final solution is to notice the contacts the change of the address.

In fact, from the analysis above, we can identify nothing useful and beneficial to the spammed. They undertake pure losses, not only the monetary, but also the psychological.

The limitation of technological and market solutions

The technical solutions to spam involve complicated mechanisms, which are not the primary concern of this paper. But the main means are filtration and blacklist. The former is used to filter the sources, headers, and content. The latter is used to mark the refused IP addresses. Practices proved that the technical filtration often misjudges, deletes, and blocks the useful and legal e-mails, and incapable to effectively stop sending of spam from the sources. At the same time, the technical solution also has influences on the transmission of the e-mail service providers and the terminals ([Taiwan Ministry of Transportation and Communications](#), p. 13). It is also possible that the recipient install filtering software to prevent spam. But it is still less effective.

In the meanwhile, spam technology and anti-spam technology are competing in

contesting with the market. The technical capacity of tracing spam source is always limited ([Taiwan Ministry of Transportation and Communications](#), p. 14). Besides the economic incentive in spamming and the technical limitation in anti-spamming, the issue is worsened by the extra costs of the service providers on improving computing ability to filter the spam, and the potential risks of misjudgment and breach of constitution. If there is no legal warrantee and liability, the possible technical solutions might also be discarded. The technical solution could be effective only when certain legal basis is ready to divide the risks between the senders, the service providers, and the recipients.

Given the technological solution is not the unique way; the legal regulations on spam are further justified by the limitation of non-legal solutions. The following analyzes the disadvantages of the non-regulatory measures.

Theoretically, the prohibition of spam could be integrated into regulations on the protection of consumers' rights. But the traditional laws can at most extend privacy protection to the activities of misuse of mail lists according to the personal data protection law, such as in Taiwan. However, this protection is limited to eight industries and cannot provide complete protection for consumers ([Taiwan Ministry of Transportation and Communications](#), p. 6).

Self-regulation is practiced by various coalitions of anti-unsolicited e-mails. The goal of these coalitions is focused on that the consumers enjoy the right to accept or refuse the bulk mails, and that the Internet resources and privacy should be sufficiently respected. The awareness of the consumers, website managers, and the Internet service providers helps to take coherent actions in combating spam, and enhancing the quality of Internet services.

Observing the current situation, we can find that the consumers' protection and self-regulation mechanisms are both less effective as well. On the contrary, the problem of spam is growing more serious. Therefore, clear rules are needed to define the scope of the spam and offer suitable punishment, neither throttling e-mail as an e-marketing tool nor leaving it as it is.

Legal regulations on spam

1. Basic approaches within the legal framework: opt-in vs. opt-out

In dealing with spam, various technological solutions are being created, used, and proved to be less effective. As a necessary remedy of the problem of the spam, legal framework must also be used to fight against spammers.

The first step in taking a legal action is to consider whether the consent of the address owner should be obtained prior to the sending of the spam message. If the prior consent is necessary, the method is called "opt-in". If the prior consent is not required, the method will be "opt-out".

The opt-in mode fully takes care of the free will in receiving messages. Through receiving e-mails, the recipients can acquire certain information. But the privacy of the recipients and the consumers must be taken into account. The right of privacy is now widely recognized and protected in constitutions and laws worldwide. Remedies for infringement of this right have also implemented through civil law or criminal law. Any potential threats to the privacy should be considered in advance of the activities. The opt-in mode might better serve this goal in the information age. Opt-in mode is adopted in Australia, China, and the European Union (for example in the United

Kingdom).³

With Directive 2002/58/EC, the European Union has adopted an "opt-in" approach for commercial communications by e-mail. The Article 13 of the Directive titled "*Unsolicited communications*" provided that:

"The use of automated calling systems without human intervention (automatic calling machines), facsimile machines (fax) or electronic mail for the purposes of direct marketing may only be allowed in respect of subscribers who have given their prior consent."

However, Article 13.2 also leaves an open door for a kind of special opt-out choice: "Where a natural or legal person obtains from its customers their electronic contact details for electronic mail, in the context of the sale of a product or a service, in accordance with Directive 95/46/EC, the same natural or legal person may use these electronic contact details for direct marketing of its own similar products or services provided that customers clearly and distinctly are given the opportunity to object, free of charge and in an easy manner, to such use of electronic contact details when they are collected and on the occasion of each message in case the customer has not initially refused such use."

Article 13.3 explicitly limits the use of unsolicited communications for purposes other than direct marketing. They are not allowed either without the consent of the subscribers concerned or in respect of subscribers who do not wish to receive these communications, the choice between these options to be determined by national legislation. This provision ensures the effective opt-out in cases the users choose to interrupt the subscription after either opt-in or limited opt-out.

The general requirements in sending commercial e-mails are by the way of ensuring the real identity, and address. Article 13.4 of the Directive prohibits the "disguising or concealing the identity of the sender on whose behalf the communication is made, or without a valid address to which the recipient may send a request that such communications cease."

The Article 13.5 of the Directive further provides that the subscriber in provision about the definition of unsolicited communications and the limited opt-out provision shall apply to natural persons. But it requires the Member States to sufficiently protect the legal interests of other subscribers.

The Directive helps to establish a legislative model within the framework of the European Union. Opt-in approach has been adopted in most EU Member States, and is under consideration in some other countries ([Sipior, Ward and Bonner](#), 2004, p. 62). Under the opt-in approach, the burden is on the senders to offer the "opt-in" option. For the e-marketing as a whole, in the case of sending in goodwill, the user can save time and costs in processing the irrelevant messages. In the case of sending mala fide, the recipients can prevent in advance. The main advantages of opt-in e-mail services are timeliness, convenience, and control.

Compared with the opt-in mode, the opt-out mode considers the difficulty of the industry in acquiring the users' written consent. If the use of such information were prohibited, the industries of financing service, direct marketing, and customer credit would be directly impacted. The advantage of the opt-out mode than written consent is that it can balance the personal privacy and right of individual consumer, offering the opportunity for consumers to express their will on whether or not to receive specific category of e-mails. The opt-out mode is adopted in Canada, Japan, South

Korea, Singapore, Taiwan, and the United States.⁴

In the North America, the United States CAN-SPAM Act superseded more than 30 state laws covering spam. The legislation adopts an opt-out approach under strict limitations. Section 5 of the Act provides the requirements for transmission of messages:

1. Prohibition of false or misleading transmission information. The Act outlaws sending commercial e-mail message, transactional or relationship message with header false or misleading information to a protected computer (Section 5 (1)). Even if the header information is "technically accurate", including the originating e-mail address, domain name, or IP address, but when they are obtained by means of false or fraudulent pretences or representations, they are regarded as "materially misleading" (Section 5 (1)(A)). If the sender "knowingly use another protected computer to relay or retransmit the message" in order to disguise the origin, the header information shall be regarded as "materially misleading" (Section 5 (1) (C)).
2. Prohibition of deceptive subject headings. The Act outlaws sending commercial message if know or should know that "a subject heading of the message would be likely to mislead a recipient, acting reasonably under the circumstances, about a material fact regarding the contents or subject matter of the message" (Section 5 (2)).
3. Prohibition of omitting return address or comparable mechanism (Section 5 (3)). The Act outlaws sending commercial e-mail message without displaying "a functioning return electronic mail address or other Internet-based mechanism" (Section 5 (3) (A)). The Act further requires that the return address or other mechanisms can be used by a recipient to opt-out by the way designated in the message (Section 5 (3) (A) (i)). The return address must be available for "no less than 30 days" after sending the message ((Section 5 (3) (A) (ii)).
4. Prohibition of transmission of commercial electronic mail after objection. In the case of opting out by a recipient, then sending e-mail more than 10 business days after the receipt of such request is unlawful (Section 5 (4)).
5. Inclusion of identifier, opt-out, and physical address in commercial electronic mail (Section 5 (5)).

The effective opt-out mechanism should be "sending once, and identifying once." It means that the messages are sent to the recipients only once if the recipients do not receive such messages any longer, and the recipients need to identify the same source of the same messages only once before he/she decide to refuse or subscribe it. Under such circumstances, mode of the users searching information changes to the mode of the users judging whether the coming information is valuable. Thus it is less wasteful for both the senders and recipients, if the senders are sending the information in goodwill.

The disadvantage of this approach is that it increases the costs of processing information in distinguishing those useful from useless, wasting work time, human resources, and money. For overall comparison of these two means, see Table 2 below.

Table 2: Comparisons between Opt-in and Opt-out (Hong Kong Information Security Website, 2005)

Approaches	Advantages	Disadvantages
Opt-in	Burden on senders to offer opt-in option. Recipients save time and costs in processing irrelevant	Malpractice of some traders. Lead to insufficient, asymmetry information, and increase costs of information searching. Malicious senders join the

	messages. Recipients prevent spam in advance.	mail lists, and send more specialized spams.
Opt-out	Burden on recipients to inform opt-out. Sending once, identifying once. Information searching changes to information selecting.	Opt-out becomes confirmation to spammer. Cost of processing information increases.

The distinction between opt-in and opt-out modes is easy to make. But in the case of opt-out mode, there exist a special case that needs a special legal answer. If the recipient of the opt-out e-mail sends back the message with selected items that he consents to receive or refuses to receive further e-mails, it is purely the purpose of opt-out. The recipient bears the expenses involved in the process. But if the recipient does not reply to the opt-out offer, the judgment of whether the recipient is willing to receive further e-mail cannot be made without an explicit legal provision. The law must give an indubitable answer.

2. Regulated scope of unsolicited message

The contents and categories of regulated unsolicited message vary among countries from each other. In the aspect of the contents of the regulated unsolicited message, countries generally target at commercial communications, such as in Australia, Japan, Korea, the United Kingdom, and the United States. The Australia Act on Unsolicited Electronic Information 2003 applies to "commercial electronic message," unless it is exempted. The Korea Act on Promotion of Information and Communication and Communications Network Utilization and Information Protection of 2001 defines unsolicited messages to advertisement information for the purpose of earning profit or commercial advertisement. The United Kingdom Privacy and Electronic Communications (EC Directive) Regulations 2003 applies to e-mail sent for the purpose of direct marketing. The United States CAN-SPAM Act defines "commercial electronic message" as "any electronic mail message the primary purpose of which is the commercial advertisement or promotion of a commercial product or service (including content on an Internet website operated for a commercial purpose)." (Section 3 (2)) Hong Kong Bill against Unsolicited Electronic Message 2005 proposes regulation on unsolicited commercial electronic message. Non-commercial message, such as the communications of governments and citizens, contribution appeal of the charity or religious organizations, communications of political parties are not limited. The provision of China Management Measures on Internet E-mail Services 2005 is wide enough to cover all kinds of e-mail messages.

In the aspect of the forms of the regulated unsolicited messages, there are also different legislations. The law in the United States limits the message to commercial e-mail. Similarly, China also limits the form of spam to e-mail. The mobile message is excluded.

Other countries adopted broad legislation to outlaw more kinds of messages. The regulated electronic message in Australia covers e-mail, instant message, and telephone. The scope of the United Kingdom law covers automatic calling system, facsimile, and e-mail. The Section 5 of Australia Spam Act 2003 defines the purpose of the Act to regulate commercial electronic message including e-mail, instant message, telephone, and similar messages. But voice calls are excluded: If a message is sent by way of a voice call made using a standard telephone service, the message is not an electronic message. Korea outlaws unsolicited e-mail, telephone, facsimile, or other media prescribed by the Presidential Decree. The term "other media" is

obviously used to cover short message service (SMS) and other electronic communications services. At the same time, Korea also specifies those messages sent to recipients in violation of law as spam (Personal Data Dispute Mediation Committee, [Korea Information Security Agency](#), 2003, p. 5-6). The Hong Kong bill covers all the unsolicited commercial electronic messages: e-mail, facsimile, instant message, and multimedia message, messages generated automatically by devices, including audio or video messages recorded beforehand and sent through the Interactive Voice Response System (IVRS) ([Xie](#), 2005).

3. Labeling of commercial e-mail

Labeling consists of displaying standard identifying labels in the subject line or header. Some countries require senders to label certain kinds of messages, but others do not require it ([Ahn](#), 2004). In order to make it possible for the e-mail service providers and the recipients to distinguish and filter the e-mails before open them, the general provision requires the sender add some words in the commercial e-mails, such as "advertisement." China requires labeling of "Advertisement" in Chinese or "AD" in English. Taiwan Draft Regulations on Unsolicited Commercial E-mail requires labeling of "Commercial," "Advertisement" in Chinese or "ADV" in English. The bill also authorizes the agency in charge of the regulation to publish other labels that can be used to identify the commercial e-mail. In Korea, Article 11 of the Ordinance of the Ministry of Information and Communication of the Act (Act on Promotion of Information and Communication and Communications Network Utilization and Information Protection of 2001) requires an "ADV" label. But in order to prohibit the irregular forms of labels such as "A*D*V" and "A~D~V", the Ordinance was revised in 2002 to exclude the irregular forms. The revision also requires an "ADLT" (adult) label if the e-mails are for adults. In June 2003, the Korea law further requires to "include the '@' (at) symbol in the title portion (right side) of any commercial e-mail address, in addition to the words 'Advertisement' or 'Adult Advertisement' as applicable." ([Korea Information Security Agency](#), 2003).

Many states in the United States require a label in the subject line of an e-mail that will alert recipients that the message is an advertisement. This includes two modes: unsolicited sexually explicit messages must contain a label of "ADV: ADULT", "ADV: ADLT", "ADULT ADVERTISEMENT", "ADV: ADULT ADVERTISEMENT" at the beginning of the subject line; unsolicited commercial e-mail messages must contain a label of "ADV:" or "ADVERTISEMENT". False, deceptive, or misleading subject lines are outlawed. Table 3 shows the different legislation modes on the problem of labeling in the United States (for a complete summary of the U.S. state laws, see [Sorkin](#), 2006).

Table 3: Legislation Modes concerning Labeling

Legislation Modes	Categories	Label	States
Requirements of Label	Unsolicited sexually explicit messages	"ADV: ADULT", "ADV: ADLT", "ADULT ADVERTISEMENT", "ADV: ADULT ADVERTISEMENT"	Alaska, Arkansas, Illinois, Indiana, Kansas, Louisiana, Maine, Minnesota, Missouri, New Mexico, North Dakota, Oklahoma, Pennsylvania, South Dakota, Tennessee, Texas, Utah, and Wisconsin

Unsolicited commercial e-mail messages	"ADV:" or "ADVERTISEMENT"	Arizona, Colorado, Michigan, and Nevada
Prohibition of False, Deceptive, or Misleading Subject Lines		Arizona, Illinois, Indiana, Kansas, Maryland, Minnesota, Missouri, North Dakota, Oklahoma, Pennsylvania, South Dakota, Texas, Washington, West Virginia, and Wyoming

In order to avoid possible disputes and damages in the direct marketing through e-mail, effective tracing of senders is critical. Laws require the sender to provide correct header of the e-mail. The Section 5 (a) (1) of United States CAN-SPAM Act, Article 3 (3) and Article 5 of Japan Specified Commercial Transactions Law for Appropriate Transmission of Specified E-mails 2002 all provide the similar requirement. The sender's identity information is also an important requirement in commercial e-mails. The Section 5 (a) (5) of the US Act, and Article 3 (2) of the Japan Law both make such provisions.

In the United States, states have taken different steps to criminalize the act of sending unsolicited commercial e-mail containing false, falsified or missing routing information, or misrepresent or obscure the point of origin or routing information; the sale, distribution, and possession with intent to sell software that is designed to falsify routing information; and unsolicited commercial e-mail using a third party's Internet address or domain name without permission. Some states require that the unsolicited commercial e-mail must include the sender's name, street address, and e-mail address, along with opt-out instructions ([Coalition Against Unsolicited Commercial Email](#), 1999). The following Table 4 compares the differences between the legislation modes of the U. S. states.

Table 4: Legislation Modes concerning Identity

Criminalization or Requirements	States
Criminalization	The act of sending unsolicited bulk e-mail containing false, falsified or missing routing information, or misrepresent or obscure the point of origin or routing information
	The sale, distribution, and possession with intent to sell software that is designed to falsify routing information
	Unsolicited commercial e-mail using a third party's Internet address or domain name without permission

Requirements	Require that the unsolicited commercial e-mail must include the sender's name, street address, and e-mail address, along with opt-out instructions	Arkansas, Colorado, Indiana, Iowa, Kansas, Maine, Minnesota, Missouri, Nevada, new Mexico, Ohio, Oklahoma, Rhode Island, Tennessee, and Utah
--------------	--	--

These different provisions within one nation indicate that the law enforcement is confronted with either the jurisdictional gap or overlap, besides possible consistency and coordination.

4. Criminal liability, administrative liability, civil liability, and international cooperation

The prohibition of spam is ensured by liability mechanisms. The liabilities for spam can take the forms of criminal, administrative and civil liabilities. In nature, the criminal liability is the most severe and deterrent one. The administrative and civil liabilities are less deterrent. But deterrence is not the only factor in determining the adoption of liabilities. The most deterrent liability might also be the most costly and thus less efficient in economic sense. Therefore, other liabilities can have comparative advantages. In either case, the international coordination and cooperation are necessary.

In some of the U.S. states, spam has been criminalized by state laws, such as Colorado, Nevada, Pennsylvania, Connecticut, Delaware, Louisiana, North Carolina, and Virginia. In some other jurisdictions without statutes regulating commercial spam, unsolicited e-mail is usually regulated with reference to harassment, stalking, and sexually explicit communication to minors, such as in Hawaii, Wisconsin, and Maryland ([Gilbert & Harrison-Watkins, 2001](#)). The Section 4 of 2004 CAN-SPAM Act prohibits using a computer without authorization to send commercial e-mail; falsifying header information in sending commercial e-mail; and registering e-mail accounts with false identifying information, and using those accounts to send commercial e-mail. Under the Act, violations of the provisions above can result in fines and imprisonment of between one and five years depending on the seriousness of the violation and other factors.

In exploring the criminal liability for spam, there are some issues deserving reconsideration.

Firstly, although the overall losses caused by spam are huge, the average loss of a single user by a single message might be very tiny. Every single user might lack the incentive to report and provide evidences to the law enforcement. If they do so, the process might involve more expenses of time, money, and energy than merely being spammed, without any expected reward. A simple reaction of users against spam might be to ignore it, until they have more sufficient psychological pulse and economic motive to report it.

Secondly, the cost of tracking down spammer is high ([Prince, 2004](#)). Although there are cases of harsh criminal sanctions, such as that a Virginian spammer was sentenced to nine years in prison for sending 10 million e-mails each day ([Wakefield, 2005](#)), the cases of large damages, such as that another spammer was sued by AOL for 7 million dollars (*Ibid*), and that a Florida-based spammer, James McCalla was imposed the uncollectible fine of 11 billion dollars for sending over 280 million unsolicited e-mail messages, and an enforceable mechanism of banning him to use the Internet for three years ([Arnfield, 2006](#)). Spamhaus estimated that spam would account for 95 percent

of all e-mails by mid-2006 ([Wakefield](#), 2004).

Thirdly, the countries adopted different legal approaches, such as opt-in, opt-out, and even no regulation at all. Within each mode, the nature and scope of the regulated messages varies from one country to another. The countries without anti-spam law neither protect the spammed nor prevent the spammer. The users become the potential targets of the spam, while the spammers might emerge in these countries or move to these countries to spam. Every country has the possibility of becoming a safe haven for spammers. This makes it less effective to coordinate internationally.

Fourthly, in addition to the high cost, and the legal and jurisdictional differences, the uncontrollability of the e-mail communications, and the trans-territorial or trans-national distribution of both the spammers and the spammed determine the very low detection and conviction probability. The traditional view supposed a more severe penalty as a more suitable deterrence. But if the probability is near zero, even the highest punishment does not work. All these factors have influence on the effectiveness of criminal liability.

In China, the regulation and punishment of spam are realized through administrative liability. The Article 24 of the Law provides that sending unsolicited e-mail, sending e-mail with false header and labeling, or sending e-mail to recipient who opt-in previously but opt-out subsequently, should be corrected under the order of Ministry of Information Industry or Bureau of Communications Management, and imposed a fine no more than 10,000 RBM Yuan (about 1,000 euros); those who obtained illegal income, should be imposed a fine no more than 30,000 RMB Yuan (about 3,000 euros).

It is also possible to take civil actions against spam senders. First of all, because the ISPs' systems are repeatedly burdened by huge volume mailings, they can incur noteworthy cost. Thus, they have the choice of seeking financial compensation through civil action. Generally, civil laws that apply to damages resulting from wrongful actions or breaches of contract would apply to conventional and online activities equally ([Ferguson & Piragoff](#), 1997).

Another form of civil action can also protect recipients from spamming. Damages are a favorable deterrent against spam. Laws in some of the U.S. states provide statutory damages to individuals and ESPs. These damages vary from 10 dollars per message in Colorado and Iowa to 500 dollars in Rhode Island.

Law enforcement needs the harmonized international actions. There have been a number of international initiatives to deal with the problem of trans-border scams. The Organization for Economic Cooperation and Development adopted new guidelines in June 2003 to promote international cooperation against trans-border fraud and deception. Recent trends in international cooperation have been between industries, organizations and the consumer or citizen, and between industries and government ([Ahn](#), 2004). Important multi-lateral organizations include the Organization for Economic Cooperation and Development, International Telecommunication Union (ITU), APEC, Internet Corporation for Assigned Names and Numbers (ICANN) and International Consumer Protection and Enforcement Network (ICPEN). In order for the international cooperation to be timely and effective, it should include various different communities ([OECD](#), 2004). In dealing with the problem of spam, the new-styled international cooperation is an urgent call. As of 2005, International Council on Internet Communications was formed to coordinate international efforts to stop spammers ([News Target](#), 2005). Given spam is still in its rapid developing stage, we cannot expect any of such institutions are able to

solve the problem in a predictable period.

International action might meet obstacles impossible to overcome. The senders and recipients in opt-in countries and the opt-out countries might first meet with unsolvable vicious cycle. The users of opt-in countries might always feel that they are annoyed by the senders of the opt-out countries. The users of the opt-out countries might feel that they are less informed by the businesses of the opt-in countries. The businesses of the opt-out countries might also feel that they are guilty of spamming users of opt-in countries. The senders of the opt-in countries might feel that they are less competitive in the e-marketing in the global market, and so forth.

Furthermore, we mentioned the different provisions of the subject line. The English-speaking countries will surely require a label in English, such as "ADV", and so forth. Other countries require a label either in their native languages or in English. This brings about little problem within one jurisdiction. The problem is that e-mail advertisements are neither language dependent nor jurisdiction dependent; laws of most countries are, nevertheless, jurisdiction dependent, protecting recipients and preventing senders in one jurisdiction. Neither are the spammers from abroad well punished, nor are the spammed from abroad well protected. Trans-national spamming is a problem that domestic laws are reluctant to deal with.

Finally, it is less possible to determine whether a message with a specific label is spam according to the domestic laws. If a Chinese sender, fully coincident with Chinese law, sends a message with a label in Chinese character to a user in Japan, who is also a Chinese citizen, he/she might identify this Chinese message as spam according to Japanese law, whether he/she consent to receive such a message or not. Because he/she receives the message in Japan, where only Japanese law applies, he/she can take an action against this Chinese sender on the basis that this message provided the irregular label.

From the above analysis, international cooperation should not only propel unified rules, but also hold spammers liable for trans-border spamming. More than ever, an international anti-spam agreement is necessary.

Concluding remarks

Spammers are motivated by greater benefits from spamming than other kind of direct mailing. The growth of spam despite the increase of efforts suggests that any previous solution cannot work alone. Comprehensive mechanisms must be established to protect the spammed and to discourage the spammer. To balance the liability among the spammer, the spammed, and the intermediaries, criminal sanctions, civil remedies, and international harmonization are all constituents of the effective legal framework.

Acknowledgements

The author would like to thank the anonymous reviewers of *Webology* for their invaluable encouragement and valuable comments on this article.

References

- Ahn, S. (2004, January 22). Background Paper for the OECD Workshop on Spam, OECD Directorate for Science, Technology and Industry Committee for Information, Computer and Communications Policy.
- Arnfield, R. (2006, January 5). [Florida Slaps Spammer with \\$11 Billion Fine](http://www.seeweekly.com/hosting-florida-slaps-spammer-with-11-billion-53252.html). Retrieved March 15, 2006 from <http://www.seeweekly.com/hosting-florida-slaps-spammer-with-11-billion-53252.html>

- Boldt, M., Carlsson, B., & Jacobsson, A. (2004). [Exploring Spyware Effects](#). Retrieved March 15, 2006, from http://psi.bth.se/mbo/exploring_spyware_effects-nordsec2004.pdf
- [Coalition against Unsolicited Commercial Email](#) (1999, December). *CAUCE News*, 3 (4). Retrieved March 15, 2006, from <http://www.cauce.org/node/110>
- Cobb, S. (2003). [The Economics of Spam](#). Retrieved March 15, 2006, from http://www.spamhelp.org/articles/economics_of_spam.pdf
- Direct Marketing Association. [Executive Summary of International Spam Laws](#). (n.d.). Retrieved March 15, 2006, from <http://www.the-dma.org/antispam/spamlaws.html>
- EquiP Technology & CipherTrust. (2004). [Spam and Productivity Theft- a Growing Concern for UK PLC](#). Retrieved March 15, 2006, from <http://www.apig.org.uk/equipandciphertrustevidence.doc>
- Federal Trade Commission (1998, July). FTC Names Its Dirty Dozens: 12 Scams Most Likely to Arrive via Bulk E-mail, FTC Consumer Alert.
- Federal Trade Commission. (2003, June 15). *National Do-Not-E-mail Report to Congress*, Author.
- Ferguson, P., & Piragoff, D. K. (1997). [Internet and Bulk Unsolicited Electronic Mail](#). Retrieved March 15, 2006, from [http://e-com.ic.gc.ca/epic/internet/inecic-ceac.nsf/vwapj/SPAM_1997En.pdf/\\$FILE/SPAM_1997En.pdf](http://e-com.ic.gc.ca/epic/internet/inecic-ceac.nsf/vwapj/SPAM_1997En.pdf/$FILE/SPAM_1997En.pdf)
- Gartner Consulting. (1999). ISPs and Spam: The Impact of Spam on Customer Retention and Acquisition, Author.
- Gauthronet, S., & Drouard, E. (2001). *Unsolicited Commercial Communications and Data Protection*. Brussels: Commission of the European Communities, Internal Market Directorate General.
- Gilber, S. & Harrison-Watkins, T. (2001). [SPAM: Survey of State and Federal Legislation](#). Retrieved March 15, 2006, from http://gsulaw.gsu.edu/lawand/papers/su01/gilbert_harrison/
- Goodman, J. T., and Rounthwaite, R. (2004). Stopping Outgoing Spam. In: *Proceedings of the 5th ACM Conference on Electronic Commerce*, 17-24 May, ACM Press, pp. 30-39.
- Goodman, P. S. (2000, December 13). Verizon Online User's E-mail Problems Persist, *Washington Post*, E01.
- Grimes, A. (2003, May 22). Digits: Spam Pays. *The Wall Street Journal*, B3.
- Hansell, S. (2003, July 29). The High, Really High or Incredibly High Cost of Spam. *The New York Times*.
- Hong Kong Information Security Website. (2005, July). [Approaches to Cope with Unsolicited Messages](#). Retrieved March 15, 2006, from <http://www.infosec.gov.hk/english/antispam/e-mail/e-mail6.htm>
- IDC (2005, February 24). [Worldwide Revenue for Antispam Solutions To Reach Over \\$1.7 Billion in 2008, IDC Reveals](#). *IDC - Press Release*. Retrieved March 15, 2006, from <http://www.idc.com/getdoc.jsp?containerId=prUS00085505>
- IMT Strategies. (2001). [Raising the Stakes in Permission Marketing](#). Stanford: Author. Retrieved March 15, 2006, from <http://www.imtstrategies.com/download/TI13.01.pdf>
- InfoWorld (2003, July). What is the Worst IT Disaster of the Last Year. *InfoWorld*.
- International Telecommunication Union (2004). *Meeting Announcement: ITU WSIS Thematic Meeting on Countering Spam*. Geneva: CICG, July 7-9.
- Kelly, J. S. (2002). [A Brief History of Spam](#). Retrieved March 15, 2006, from <http://www-106.ibm.com/developerworks/linux/library/l-spam/l-spam.html>
- Khong, W. K (2001, October). [The Law and Economics of Junk E-mails](#)

([Spam](#)). Retrieved March 15, 2006, from <http://www.frg.eur.nl/rile/emle/Theses/Khong.pdf>

- Khong, W. K. (2004). An Economic Analysis of Spam Law. *Erasmus Law and Economics Review*, 1 (February), 23-45.
- Korea Information Security Agency (2003). [Korea Spam Response Center-Legislation for Anti-Spam Regulations: Mandatory Indication of Advertisement](#). Retrieved March 15, 2006, from http://www.spamcop.or.kr/eng/m_2.html
- Korea Information Security Agency, Personal Data Dispute Mediation Committee (2003). *Introduction to Act Related to Spam in Korea*, Author.
- Libbenga, J. (2005, July 21). [Biggest 419 Bust in History](#). Retrieved March 15, 2006, from http://www.theregister.co.uk/2005/07/21/scammers_nabbed/
- Living Internet (2005, June 6). [E-mail Spam](#). Retrieved March 15, 2006, from http://www.livinginternet.com/e/et_spam.htm
- Mail Abuse Prevention System (2004). [Definition of Spam](#). Retrieved March 15, 2006, from <http://www.mail-abuse.comSpam-def.html>
- Midnet Media (2003). [Economics of E-mail](#). Retrieved March 15, 2006, from <http://www.midnetmedia.com/BUILD/PDF/MMPG4.pdf>
- Moran, J. M. (2002, June 30). Spam King Living High in the Bayou. *The Hartford Courant*.
- News Target (2005, April 28). [New International Anti-Spam Council Pledges to Fight Spam around the World](#). Retrieved March 15, 2006, from http://www.wired.com/news/technology/0,1282,64383,00.html?tw=wn_tophead_5
- Niall, J. (2000). *The E-mail Marketing Dialogue*. Cambridge: Forrester.
- OECD (2003). *OECD Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices Across Borders*, Author.
- OECD (2004). *Second OECD Workshop on Spam: Report of the Workshop*, Author.
- PC World (2003, August 29). [Sobig May Be Working for Spammers](#). Retrieved March 15, 2006, from <http://www.pcworld.com/news/article/0,aid,112261,00.asp>
- Peppers, D. & Rogers, M. (2000). *E-mail Marketing Maximized*. Stanford: Peppers.
- Prince, M. (2004). [How to Craft an Effective Anti-Spam Law](#). June. Retrieved March 15, 2006, from <http://www.itu.int/osg/spu/spam/>
- Radical Group (2005). *The Radical Group, Inc. Release Q1 2005 Market Numbers Update*, Author.
- Sadowsky, G., Dempsey, J. X., Greenberg, A., Mack, B. J., and Schwartz, A. (2003). *Information Technology Security Handbook*. The International Bank for Reconstruction and Development.
- Sandiego Media (2005). [E-mail Marketing Solution](#). Retrieved March 15, 2006, from http://www.sandiegomedia.com/cgi-bin/main/co_disp/displ/strfnbr/101/pgname/e-mail_marketing_benefits
- Simon, H. A. (1982). *Designing Organizations for an Information-Rich World: Models of Bounded Rationality*. MIT Press.
- Sipior, J. C., Ward, B. T., & Bonner, P. G. (2004, June). Should Spam Be on the Menu? *Communications of the ACM*, 47 (6), 59-63.
- Sorkin, D.E. (2006). [Spam Laws](#). Retrieved March 15, 2006, from <http://www.spamlaws.com>
- Taiwan Ministry of Transportation and Communications, The Directorate General of Telecommunications (2005). Questions and Answers on Relevant Topics about Draft Regulations on Unsolicited Commercial E-mail. Retrieved March 15, 2006, from <http://www.dgt.gov.tw/chinese/ncc/mail-regulation>

/ncc-SPAM-Q&A-940215.doc

- TopTenReview (2005). What Makes a Great Internet Filter Software Solution? Retrieved March 15, 2006 from <http://internet-filter-review.toptenreviews.com>
- Templeton (2003). Origin of the Term "Spam" to Mean Net Abuse. Retrieved March 15, 2006, from <http://www.templetons.com/brad/spamterm.html>
- Wakefield, J. (2005, April 21). UK Laws Are Failing to Deter Spam. *BBC News*. Retrieved March 15, 2006, from <http://news.bbc.co.uk/1/hi/technology/4466053.stm>
- World Summit of Information Society (2003). *Declaration of Principles-Building the Information Society: A Global Challenge in the New Millennium*, Author.
- Wreden, N. (1999, January 9), Mapping the Frontiers on E-mail Marketing. *Harvard Management Communication Letter*, 6-8.
- Wright, N. D., & Bolfing, C. P. (2001). *Marketing via E-mail: Maximizing its Effectiveness without Resorting to Spam*. James Madison University.
- Xie, T. (2005). Comments on Hong Kong Bill against Unsolicited Electronic Message". November 21, 2005. Retrieved March 15, 2006, from <http://www.chinaeclaw.com/News/2005-11-21/4904.html>
- Zeller, T., Jr. (2005, February). Law Barring Junk E-mail Allows a Flood Instead. *The New York Times*, A1.

Footnote

1. See Living Internet (2005) for details of the message.
2. The invisible hand is a metaphor created by Adam Smith to illustrate the principle of "enlightened self interest".
3. See Australia SPAM Act 2003; China Management Measures on Internet E-mail Services 2005, Article 13 (2) and (3), and Article 14; European Directive 2002/58/EC; and the United Kingdom Privacy and Electronic Communications (EC Directive) Regulations 2003.
4. See Canada Personal Information Protection and Electronic Documents Act (2000, c. 5); Japan Specified Commercial Transactions Law for Appropriate Transmission of Specified E-mails 2002; Korea Act on Promotion of Information and Communication and Communications Network Utilization and Information Protection of 2001 (revised December 18, 2002); Singapore Proposed Legislation Framework on Controlling Unsolicited E-mail (Singapore Information Development Agency and Singapore Department of Justice); Taiwan Draft Regulations on Unsolicited Commercial E-mail; the United States CAN-SPAM Act (Controlling the Assault of Non-solicited Pornography and Marketing Act 2003) 2003.

Bibliographic information of this paper for citing:

Li, X. (2006). "E-marketing, Unsolicited Commercial E-mail, and Legal Solutions." *Webology*, 3(1), Article 23. Available at: <http://www.webology.org/2006/v3n1/a23.html>

This article has been cited by other articles

Copyright © 2006, Xingan Li

The Phenomenon of Unsolicited E-mails with Attachments

Xingan Li

University of Turku

ABSTRACT

Unsolicited e-mails became prevalent with the growing penetration of computer networks. The senders of unsolicited e-mails make every effort to get the attention of the recipient. The goal is for their messages and/or attachments to be opened. The victimization of recipients of unsolicited messages with attachments happens without the recipients actually accessing their e-mail accounts. The victimization-conspiracy model happens when the messages include contents offering products or services that need illegal involvement of the recipients. The recipients of messages with such offers are first victimized by the unsolicited messages; and if they accept the illegal services or purchase the illegal products, they are likely to become the co-conspirators of the senders. The senders and the recipient would reach an illegal double win effect. The unsolicited messages with attachments provide e-mail users many different options. The majority of messages in this study, however, offered recipients two alternatives; to conspire in tax evasion, or to be damaged by viruses.

Introduction

The open access of the Internet to commercial users at the end of the twentieth century created a new path to social life in this era. As of 2005, more than 683 million e-mail users hold 1.2 billion accounts (Radical Group, 2005), utilizing this unprecedented means of communication and marketing on a daily basis. Unsolicited e-mails have become a nuisance that every computer and internet user must deal with. The recipients' property rights, fair trade, public morals, cybersecurity, data protection, and other content-related and goods-related transgresses and offences are all challenges that society is confronted with (Li, 2006). The unsolicited e-mails can cause disruption of information transmission, commercial transaction, military operation, education, and recreation.

Many studies have been done to explore the phenomenology of unsolicited commercial e-mail (UCE, or unsolicited bulk e-mail, UBE, or simply spam). Others have dealt particularly with the costs and benefits for both senders and recipients that is derived from the unsolicited e-mail (Khong, 2001, 2004), the overall impact on productivity of individual employees and enterprises (Nucleus, 2003, 2004), the scale and volume of unsolicited e-mail (Radical Group, 2005), the impact on a consumers' attitude and their confidence towards e-commerce (TACD, 2003; Fallows, 2003; Harris Interactive, 2003), the higher possibility of receiving unsolicited e-mail due to online-published addresses (Federal Trade Commission, 2002b), the ignorance of removal requests by senders (Federal Trade Commission, 2002a), and the technical and legal solution on unsolicited e-mail (Sorkin, 2001).

Few studies, however, have dealt with unsolicited e-mails with attachments, particularly the degree of risk a single e-mail user might be confronted with. In this study, I use a sample of 501 unsolicited e-mails with attachments, first presenting the analysis of the types of sender column, types of subject column, types of offers in message content, and types, sizes and nature of attachments to these messages. Hereinafter the term "spam" is deliberately avoided by the author, due to the lack of a universally-accepted unified definition. The author prefers the phrase "unsolicited e-mail" without the modifier "commercial", in order to enlarge the coverage of messages with attachments in this study to virus spreaders.

Literature Review

The increased capability of computers and networks to process information, causes a "wealth of information" and can lead to "poverty of attention" (Simon, 1982). Unsolicited bulk e-mail

(UBE) or unsolicited commercial e-mail (UCE) represents an example of the superfluous information that e-mail users must deal with and do not expect to consume. Unsolicited e-mail brings about the negative image of e-marketing; frightening e-mail users from trusting e-mail communications.

Unsolicited e-mails sent to multiple recipients can have broad negative effects on e-mail marketing. An increasing number of e-mails are never read by the recipients, and the users prefer limiting or disrupting the business contacts (Karnell, 2002). The prevalence of unsolicited messages demonstrates a growing threat to the information society (World Summit on the Information Society, 2003, paragraph 37).

A few studies disclosed the spamming behaviour by narrative discourse about the reasons and methods of spamming, revealing the wisdom of defeating anti-spam techniques, avoiding being identified, and escaping the law (Spammer-X, 2004). Some also described the world of the spammers and spam-fighters, giving information on the mechanisms of spamming and spam fighting (McWilliams, 2005). Others presented the most usual spam traps and explained why the current solutions are ineffective (Goodman, 2004). Efforts have also been made to analyse a wide variety of e-mail in order to produce a profile of spam and develop a profile of the spammers (Lambert, 2003).

Unsolicited e-mails usually involve multiple scams. A dozen of the most likely spam scams have been identified, They cover spam and scams from business opportunities to quick money, working at home, guaranteed loans, and so on (Federal Trade Commission, 1998).

Besides direct victimisation, unsolicited e-mails have other indirect effects on productivity. An average of 13.3 unsolicited messages reached the employee per day; each employee then spent an average of 6.5 minutes per day dealing with the unsolicited messages. These unsolicited messages caused an average of 1.4 percent in productivity loss per employee per year, equal to an average cost of 874 dollars per employee per year (Nucleus, 2003).

Although it is difficult to measure the costs and benefits of spamming, if the benefits obtained from the spamming outweigh the cost, then the spammer will likely undertake the spamming activity (Khong, 2004). It follows that if there is one successful commercial transaction, the spammer can realize his or her benefit. The costs that are involved in spamming can be roughly estimated according to the costs of bandwidth, message sending, and obtaining of the recipients address. The costs of bandwidth and message sending are minimal. According to Sadowsky (2003, p. 55), the spammer can obtain users' e-mail address in the 13 situations. Obviously, the most convenient and least expensive way is to harvest e-mail addresses automatically with specific software. The software is also available from Internet, either being free of charge or with an inexpensive price.

The revenue of spammer from sending message has been found high in a few studies Goodman and Routhwaite (2004). The concept of "the parasitic economics of spam" was proposed, meaning that the act of sending a message costs the sender less than it costs all other parties impacted by the sending of the message (Cobb, 2003, p. 2).

The cost and benefit of the spamming can also be estimated. The costs created by spam can be far reaching. They include the waste of the users' time, bandwidth and storage, anti-spam solutions, and overloading at the mailbox (Gauthronet and Drouard, 2001). The average amount of time and money lost in processing a single message might not be significant. However, theoretically, the loss of time and money in aggregate in dealing with these messages might be huge (Li, 2006). Spam also induces costs of the bandwidth and storage, losses due to interruption of services, and anti-spam solutions (Gauthronet and Drouard, 2001). The interruption of service is unfortunate for both the provider and user causing losses in business and confidence. Worldwide revenue for anti-spam solutions will exceed 1.7 billion dollars in 2008 (IDC, 2005). If the e-mail address has ever been put on the institution's Web site, or personal homepage, it is highly possibly that the address will be harvested, sold, and abused by senders (Federal Trade Commission, 2003b).

Unsolicited e-mail is almost never useful or beneficial to the recipient. Based on data from previous studies, it is reasonable to conclude that the recipients of unsolicited e-mail are at risk for both monetary and psychological losses (Li, 2006).

Worse yet, the number of unsolicited e-mails are increasing. Users received an average of twice the number unsolicited messages from the previous year, with an average 3.1 percent of productivity loss in 2004. The ability of technical solutions to unsolicited messages became less effective (Nucleus, 2004).

A long-term side effect of increasing unsolicited e-mails is that they cause some e-mail users to use e-mail less, and trust the online environment less. Fear of unsolicited messages increased (Fallows, 2003).

Although many regulatory methods have been implemented, and some of the messages seem to follow the rules, most removal links or addresses were dead or did not function, attempts to send reply e-mail messages were also unsuccessful (Federal Trade Commission, 2002a).

About 66 percent of spam messages are fraudulent in the “from” or subject columns, or in the message itself (Federal Trade Commission, 2003a). These false advertisements might distort the normal market of goods and services, harm the normal trade order, or reduce consumers’ confidence (The Directorate General of Telecommunications Ministry of Transportation and Communications, 2005, pp. 6–7). The large volume of spam, malicious programs and malicious linkages contained in the messages, are the main threats (PC World, 2003).

Anti-spamming techniques that are inadequate and regulations that are ineffective, have created a phenomenon of unsolicited e-mails developed with spam techniques. Web pages, newsgroups, and chat room are all attractive to unsolicited message senders for harvesting e-mail addresses (Federal Trade Commission, 2002b). Spammers continue to harvest e-mail address posted on web sites, and to a much lesser extent, those posted on blogs and USENET groups. Masking email addresses when posting on web sites can substantially reduce the risk of harvesting (Federal Trade Commission, 2005). Many spammers send their messages by unauthorized use of other individuals or organizations’ accounts (Organization of Economic Cooperation and Development, 2004). E-mail address harvesting software can collect this information automatically from web pages (Boldt, Carlsson and Jacobsson, 2004, p. 8). Based on the discussions of spy ware and on the findings from the two experiments, spy ware has a negative effect on computer security and user privacy. Spy ware enables for the spreading of e-mail addresses that may result in the receiving of unsolicited e-mail (Boldt, Carlsson and Jacobsson, 2004, p. 4).

Most online adults reported that they received more spam compared with six months earlier. Only 14 percent have seen a decline in the volume of spam. A majority of respondents reported unsolicited messages to be annoying or very annoying (Taylor, 2003).

Much has been done about the phenomenon of unsolicited e-mail. In this systematic discourse, there is an apparent silence about specific messages with attachments. This study will not begin with a description of the importance of studying such messages, but will directly sketch an overall picture of this phenomenon. Attachments pose problems other than messages themselves and deserve more observation. This study is looking at unsolicited e-mails with attachments by analysing a sample. The following section will briefly introduce the methodology.

Methodology

This article presents a case study on unsolicited e-mails with attachments, analysing the sender column, subject column, content and attachments of these messages. The sample was composed of 501 messages with attachments in about 25,960 unsolicited e-mails in one e-mail account collected during a 12-month period from June 2005 to May 2006.

In analysing each message, it is necessary to establish a standard to categorise the messages into different types according to their sender column, subject column, content and attachments. The standard to

decide if the sender column is proper is the name format. Personal names composed of “first name” and “surname” are considered proper, regardless of their order. The name for an organization is also easy to judge by comparing the name in the sender column with what appears in the content. If they are consistent with each other, and are reasonable names, then, they are counted as proper.

The standard for deciding whether a subject column is proper has been loosely defined. Because there is only one message labelled with an “AD:” label, in strict sense all the subject columns of other messages are improper. However, the emphasis of this paper is not to coincide with the legal standard. Rather, it is focused on the analysis of the phenomenon of unsolicited e-mails with attachments. The message with “AD:” label and messages with words explaining the content or consistent with the content are regarded as proper. All other messages where the subject column is inconsistent with the content is considered improper.

The content is categorised according to the offers provided, including products, financial, adult, IT-related, health, scam and fraud, leisure, political, spiritual, and other. But in this sample, financial, adult, health, scam and fraud, leisure, spiritual offers are not as significant as many other studies revealed. They are put into “other services.”

Findings

Types of File Formats of Attachments

Out of 501 messages with attachments, three attachments were missing. Other attachments are comprised of 14 kinds of document formats. Nearly forty percent of the attachments are “zip” or “rar” format compressed files, mostly viruses, which represent the most severe threats to the e-mail users’ computer security. Approximately one third of the total attachments are files of various image formats, including “gif,” “jpg,” and “scr.” Another one third of the attachments are files of various document formats, including “chm,” “doc,” “htm,” “txt,” and “xls.” These two categories are relatively virus-free, but include annoying contents and hyper links. These three categories constitute more than 94 percent of all attachments. Another less frequent category is files in executable file formats, including “exe” and “com.” accounting for 4.4 percent of all attachments.

In these file formats, files with filename extensions of “zip” and “rar” are more dangerous. All the other files types can be “opened” with some kind of programs upon download and the contents can be read in the case of documents, viewed in the case of images, listened to in the case of audio, or simply ignored in the case of executable programmes which may involve greater danger than other files. But it’s well known that the types of original files included in compressed files have to be opened by uncompress programmes, and then the unzipped files can be opened by other application programmes. The real danger does not come from files other than “zip” and “rar” because if people know the real type of the original files they can determine whether or not to open the files. The “zip” and “rar” files are much more devious. In fact, files concealed with the filename extensions of compressed files are usually not compressed files, but are executable programmes. Therefore, when users execute the first step and they think they are unzipping the file, they are actually activating the malicious programme. In fact, most virus-spreading messages are camouflaged in this manner.

Table 1. Types of file formats of attachments

Type of file format	Number	Percentage
Compressed (*.zip and *.rar)	195	38.9
Text based (*.chm, *.doc, *.htm, *.txt, and *.xls)	142	28.3
Image based (*.gif, *.jpg, and *.src)	117	23.4
Executable (*.com and *.exe)	22	4.4
Other	25	5
Total	501	100

Table 2. Sizes of messages with attachments

Size	Number	Percentage
<100kb	446	89.0
100–200kb	11	2.2
>200kb	44	8.8
Total 23,765kb	501	100

In unsolicited e-mails with image attachments, the content of the e-mail is concealed in images and displayed in the messages, thus the sender avoids the detection and blocking by text-based filters. In some cases, attachments also contain animated images that make it more difficult for spam filters to work.

Sizes of Messages with Attachments

The average size of the messages with attachments was 47.44kb. Approximately 90 percent of the messages with attachments were smaller than 100kb. Only 2 percent of these messages are between 100–200kb. Nearly 9 percent of the messages are bigger than 200kb. In fact, about 285 messages, which constitute more than half of the messages with attachments, are smaller than 30kb. The messages with the sizes of 1kb and 2kb alone, account for more than 28 percent of the sample. They are mostly empty “zip” files, with the possibility of attachments containing viruses that may have been disinfected by the e-mail service provider. The messages with attachments spreading W32.netsky.C@mm (35kb) and W32.Sober.X@mm (75kb) viruses account for 16 percent and 7 percent of all of the messages respectively.

A majority of attachments are smaller than 200kb, a size that a majority of most dangerous viruses, worms, Trojan Horses, or other malicious programmes take. Most viruses are small in size, yet extremely harmful. That's why they are so suitable to be spread by e-mail attachments.

Unsolicited messages with attachments account for less than 2 percent of all unsolicited messages. The average size of unsolicited e-mails with attachments is 47.44kb, compared with the average size of 7.32kb for other unsolicited e-mails, 6.5 times larger. In fact, unsolicited messages with attachments contribute to more than 10 percent of the average size of all unsolicited messages, enlarging the average size from 7.32kb of unsolicited messages without attachments to 8.09kb of all of the unsolicited messages.

Many people claim that unsolicited e-mails consume large amount of internet bandwidth. It is clear that messages with attachments are even more harmful than those without. Unsolicited e-mails with attachments are likely to cause even greater bandwidth problems. The increasing size and number of unsolicited e-mails will likely cause additional operating cost in server processing time and storage capacity.

Types of Sender Column in Unsolicited Messages with Attachments

Among the 501 messages with attachments, one had a blank sender column. Senders of unsolicited messages with attachments tend to hide their names but show their e-mail addresses, proper or not. Approximately 60 percent of all messages show e-mail addresses instead of the senders' name, which should be considered improper. Others conceal their names with their surnames and titles, meaningless letters and numbers, describing their offers (products, services and activities), filled with words inducing users to open the messages, or simply exploiting recipients' names and e-mail address. Approximately

Table 3. Compare of average sizes of messages

Item	Total size	Number	Average size
Average size of unsolicited e-mails with attachments	23,765kb	501	47.44kb
Average size of other unsolicited e-mails	186,254kb	25,459	7.32kb
Average size of all unsolicited e-mails	210,019kb	25,960	8.09kb

Table 4. Types of sender column in unsolicited messages with attachments

Type	Number	Percentage (/501)
Proper	124	24.8
Improper	377	75.2
Total	501	100

Table 5. High ratio of proper sender column in unsolicited message with attachments

Type of offer	Number of proper sender column	Percentage
Political	14	56
Quick money	1	50
IT related	33	70.2
Tax evasion	37	53.6
Employment	6	60

three quarters of the messages bear improper sender columns. About one quarter of the messages bear proper personal names or company names.

The improper sender columns include the following: blank, product descriptions, services and activities, meaningless letters and numbers, recipients' name and address, recipients e-mail address or surname plus title. These are all methods used to avoid showing sender names. As Khong (2001) pointed out,

"Because of flames and mail bombs from angered spam recipients, many spammers do not use valid email addresses in their spam. However, this causes difficulties for spam recipients to contact the spammers in order to request not to be spammed in the future." (p. 24)

In different types of offers the proportion of messages with proper sender column are different. Messages providing political propaganda, quick money, IT related products and services, tax evasion and employment have a high ratio of formal sender column.

Table 6. Types of subject column in unsolicited messages with attachments

Type	Number	Percentage
Proper (with "AD:" label)	1	0.2
Improper	500	99.8
Pretending as contacts	202	40.4
Describing message content	117	23.4
Pretending as service provider	84	16.8
Misleading statements	74	14.8
Other	23	4.6
Total	501	100

Table 7. Types of content of messages with attachments

Type	Number	Percentage
Virus	141	28
Products	109	21.8
Empty attachments	103	20.6
Tax evasion	69	13.8
IT related	29	5.8
Political	25	5
Other services	25	5
Total	501	100

Table 8. Consistency of contents with attachments

Type	Number	Consistency number	Consistency percentage within the category
Virus	141	0	0
Products	109	95	87.2
Empty attachments	103	0	0
Tax evasion	69	69	100
IT related	29	24	82.8
Political	25	25	100
Employment	14	11	78.6
Other services	11	5	45.5

Types of Subject Column in Unsolicited Messages with Attachments

In order for the filtering techniques to automatically identify and block unsolicited e-mails, laws in some countries require that the senders use particular labels in the subject column. To label the subject column with “AD:”, “ADV:”, or any other kinds of regulatory means, however, is a legislative invention that has never been respected by senders of unsolicited messages. Only less than two in one thousand messages have fulfilled this requirement. Two in one hundred of the messages with attachments left the subject column blank. Approximately 15 percent of messages used misleading statements to confuse the recipients. All others attempted to draw recipients’ attention and attract them to open the messages, furnished the subject column with languages describing the content, giving greetings, appearing related to users’ e-mail service, bearing “Re:” and “Fw:” labels, or pretending to be the recipients friend, etc.

Proper Subject Column in Unsolicited Messages with Attachments

Almost all of the senders of messages with attachments offering information on human resources recruitment, companies or websites, publishing, printing, card manufacture, etc., sales of health products, clothes, and tax evasion displayed the proper subject column. A high percentage of providers of telecommunications services, sellers of books, VCDs, and DVDs, training information providers, quick money information providers, and providers of other services provided proper subject columns in their messages. All the senders of other messages were reluctant to provide proper subjects for their potential recipients.

Types of Content of Messages with Attachments

More than 28 percent of messages are designed to spread viruses. More than one in five offers various products. More than one in five contained empty attachments. Messages offering tax evasion services constitute about 10 percent. The messages offering telecommunications services, political propaganda, and other services constitute around 5 percent separately. Interestingly, there are rarely any messages containing attachments involving adult content, investment chances, sales of pirated software, or other common offers frequently mentioned in other studies.

Table 9. Types of contact method provided in unsolicited messages with attachments

Contact Method	Number	Percentage (/501)
Traditional communications	50	10
Telecommunications	451	90
E-mail address	113	22.6
Fax number	79	15.8
Instant online chat	52	10.4
Mobile phone	112	22.4
Telephone	145	28.9
Website	182	36.3

Table 10. Proper and improper sender and subject columns and content

Item	Character	Number	Percentage
Sender	Proper	100	20
	Improper	401	80
Subject	Proper	166	33.1
	Improper	335	66.9
Content	Proper	260	51.9
	Improper	241	48.1

Consistency of Contents with Attachments

Interestingly, most messages have a high percentage of content consistency. The exceptions are messages with empty attachments and messages with attachments that spread viruses. In both these cases, the senders bypass technical filters and artificial judgments using different methods.

Types of Contact Method Provided in Unsolicited Messages with Attachments

Because many unsolicited messages with attachments are spreading viruses, they generally provide no contact information. However, there are a few exceptions. Other messages included one or more kinds of contact methods in the message texts. Out of 501 messages analyzed, more than one-third of the messages provided hyperlinks to websites, while less than one-third provided telephone numbers. Both e-mail addresses and mobile phone numbers are preferred by more than 22 percent of senders. Fax numbers and physical addresses are included in about 16 and 10 percent of messages respectively. Instant online chat systems, such as MSN and QQ, are provided in 10.4 percent of messages.

Unsubscribe is nothing more than a decoration in unsolicited messages with attachments. Unsubscribe methods are only provided in 2.2 percent of the messages. The usual method is to provide a URL link at the bottom of the messages for the recipients to click on. In the opened links, the recipients can access web pages where they can choose to unsubscribe. Some unsubscribe methods require the recipients to send e-mails to specific addresses. The users of unsolicited messages in this study have never subscribed any of the messages with attachments. These messages can all be viewed as opt-out e-mails. Most of the unsubscribe methods do not work effectively. In extreme cases, the link simply connects the recipient to a webpage requiring a fresh registration. This gives the impression that the sender's real intent is to obtain the recipient's profile, not to unsubscribe them at all.

Improper Sender, Subject and Content Column

One in five of the unsolicited messages with attachments used a proper format in the sender column, one in three used proper subject column, and more than half provided proper content. However, only 58 messages had both proper format of sender and subject columns, and 293 messages had both improper sender format and subject column. Another 42 messages had the proper sender column format but they contained an improper subject column format, while 108 messages had an improper sender column format while utilizing a proper subject column format. The overall percentage of messages with improper subject or sender columns constituted 88.4 percent.

Conclusions

From the findings of this study, like in other unsolicited e-mails, the senders of unsolicited e-mails with attachments make every effort to gain the attention of the recipient. Their main goal is for their messages and/or attachments to be opened. Generally, they use informal, irregular and illegal forms of sender and subject columns, but ensure the contents are consistent with their real intent (except messages spreading viruses) to demonstrate their offers and continue their scams.

The surveyed messages with attachments prove that, except messages spreading viruses, they are relatively moderate in the sense of harmfulness of the contents, compared with the findings in previous studies which did not distinguish between messages with attachments from those without.

In principle, the victimization of recipients of unsolicited messages with attachments happens without the actual access of the recipients to their e-mail accounts. The victimization means that their e-mail accounts are being spammed, whether they open their accounts or not. Under current legal framework, the receiving of unsolicited messages is sufficient to constitute victimization.

The victimization-conspiracy model happens when the messages include contents offering tax evasion services, transaction of unauthorised duplicated software, transaction of falsified documents, and so on. The recipients of messages with such offers are first victimized by the unsolicited messages; and if they accept the illegal services or purchase the illegal products, they are likely to become the co-conspirators of the senders. This study does not cover further exploration into the practical effects of such conspiracy, but the messages provide potential risks for the recipients to engage in the activities.

Because the recipients of the unsolicited messages inducing conspiracy in an illegal activity would expect to benefit from the cooperation with the senders, the senders are more likely to send these kind of messages. The senders and the recipient would reach an illegal double win effect. This phenomenon will have a profound impact on the development of deviant behaviour.

In addition, the unsolicited messages with attachments provide e-mail users many different options, either legitimate or illegitimate, either to conspire or to be further victimized by attached viruses or pre-established scams. The majority of messages in this study, however, offered recipients primarily two alternatives: to conspire in tax evasion, or to be damaged by viruses, because the character of these two kinds of messages deserves special observation.

In the case of conspiracy in tax evasion, the senders always provide valid contact methods so as to induce the recipients to participate in the illegitimate operation. The offer seemingly aims to establish a trust relationship between service provider and clients. But the effect is that they form a conspiracy. The recipients have to react actively before they become the co-conspirators of the tax evasion activities. The process might involve repeated e-mail exchanges after the initial unsolicited message. Under these circumstances, the unsolicited messages might be transformed into literally valuable (but morally wrong and legally prohibited) information. Thus the recipients might be less likely to reject such messages. Such messages become the communication means for the trespassers and criminals, posing a great threat to the social control over illegal activities.

In the case of viruses attack, the senders exploit social engineering to induce the recipients to open the messages and subsequently the attachments, by blurring the sender, subject columns and falsifying the message contents and attachment names. These messages do not require replies from the recipients before they cause damage. They are also dangerous for the recipients in the sense that they are likely to destroy hardware and software, devastate human resources, and obstruct business.

It is noteworthy to point out that the scale of this study is minimal, but the object of the study is important. For a better understanding of this phenomenon to be achieved, future studies can do more: adopting a bigger sample, incorporating content analysis, and conducting interviews with victims and perpetrators.

I would like to thank the anonymous reviewers, who contributed comments and recommendations on the initial version of this paper, which led to its overall improvement.

COLUMBIA ONLINE CITATION: HUMANITIES STYLE

Xingan, Li. "The Phenomenon of Unsolicited E-mails with Attachments." *Studies in Media & Information Literacy Education*, 7.2 (2007).

<http://www.utpress.utoronto.ca/journal/ejournals/simile> (insert access date here).

COLUMBIA ONLINE CITATION: SCIENTIFIC STYLE

Xingan, L. (2007). The Phenomenon of Unsolicited E-mails with Attachments. *Studies in Media & Information Literacy Education*, 7(2).
<http://www.utpress.utoronto.ca/journal/ejournals/simile> (insert access date here).

BIOGRAPHICAL NOTE

Li Xingan is currently a LL.D. student at the University of Turku, Finland. He holds a LL.B. from Inner Mongolia University in Huhhot, and a LL.M. from China University of Political Science and Law in Beijing. His research interest involves the criminal phenomenon related to the information system.

AUTHOR CONTACT INFORMATION

Li Xingan
 University of Turku
 Faculty of Law
 20014 Turun Yliopisto
 Finland
 E-mail: xingan.li@yahoo.com

References

Boldt, M., Carlsson, B., & Jacobsson, A. (2004). Exploring Spyware Effects. Retrieved 31 May 2006, from http://psi.bth.se/mbo/exploring_spyware_effects-nordsec2004.pdf

Cobb, S. (2003). The Economics of Spam. Retrieved 31 May 2006, from http://www.spamhelp.org/articles/economics_of_spam.pdf

Fallows, D. (2003, October). Spam: How It Is hurting E-mail and Degrading Life on the Internet. Retrieved 31 May 2006, from http://www.pewinternet.org/pdfs/PIP_spam_Report.pdf

Federal Trade Commission (1998, July). Federal Trade Commission Names its Dirty Dozens: 12 Scams Most Likely to Arrive via Bulk E-mail, *Federal Trade Commission Consumer Alert*.

Federal Trade Commission (2002a, April). *Remove Me Surf*.

Federal Trade Commission (2002b, November). *E-mail Address Harvesting: How Spammers Reap What You Sow*.

Federal Trade Commission (2003a, April). *False Claims in Spam: A Report by the Federal Trade Commission's Division of Marketing Practices*.

Federal Trade Commission (2005, November). *Email Address Harvesting and the Effectiveness of Anti-Spam Filters: A Report by the Federal Trade Commission's Division of Marketing Practices*.

Federal Trade Commission. (2003b, June 15). *National Do-Not-E-mail Report to Congress*.

Gauthronet, S., & Drouard, E. (2001). *Unsolicited Commercial Communications and Data Protection*. Brussels: Commission of the European Communities, Internal Market Directorate General.

Goodman, D. (2004). *Spam Wars: Our Last Best Chance to Defeat Spammers, Scammers & Hackers*. New York, New York: SelectBooks.

Goodman, J.T., & Routhwaite, R. (2004). Stopping Outgoing Spam. In *Proceedings of the 5th ACM Conference on Electronic Commerce*, 17–24 May, ACM Press, 30–39.

IDC (2005, February 24). Worldwide Revenue for Antispam Solutions to Reach Over \$1.7 Billion in 2008, IDC Reveals. *IDC - Press Release*.

Karnell, J. (2002). Raising the Stakes in Permission Marketing. Retrieved 31 May 2006, from <http://www.onetooneinteractive.com/resource/whitepapers/0003.html>

Khong, W.K. (2001, October). The Law and Economics of Junk E-mails (Spam). Retrieved 31 May 2006, from <http://www.frg.eur.nl/rile/emle/Theeses/Khong.pdf>

Khong, W.K. (2004). An Economic Analysis of Spam Law. *Erasmus Law and Economics Review*, 1(February), 23–45.

Lambert, A. (2003, September). *Analysis of Spam*. Master of Science in Computer Science Dissertation. Dublin: University of Dublin.

Li, X. (2006). E-Marketing, Unsolicited Commercial Electronic Mail, and Legal Regulations, *Webology*, 3(1), 2006.

McWilliams, B. (2005). *Spam Kings*, Sebastopol: O'Reilly Media.

Nucleus (2003). *Spam: The Silent ROI Killer*, Research Note D59.

Nucleus (2004). *Spam: The Serial ROI Killer*, Research Note E50.

Organization of Economic Cooperation Development (2004). *Second Organization of Economic Cooperation and Development Workshop on Spam: Report of the Workshop*.

Organization of Economic Cooperation Development (2003). *Organization of Economic Cooperation and Development Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices Across Borders*, Author.

PC World (2003, August 29). Sobig May Be Working for Spammers. Retrieved 31 May 2006 from <http://www.pcworld.com/news/article/0,aid,112261,00.asp>

Radical Group (2005). *The Radical Group, Inc. Release Q1 2005 Market Numbers Update*.

Sadowsky, G., Dempsey, J.X., Greenberg, A., Mack, B.J., & Schwartz, A. (2003). *Information Technology Security Handbook*. The International Bank for Reconstruction and Development.

Simon, H.A. (1982). *Designing Organizations for an Information-Rich World: Models of Bounded Rationality*. Massachusetts: Massachusetts Institute of Technology Press.

Sorkin, D.E. (2001). Technical and Legal Approached to Unsolicited Electronic E-mail. *University of San Francisco Law Review*, Vol. 35, pp. 325–384. Retrieved 31 May 2006, from <http://www.sorkin.org/articles/usf.pdf>

Spammer-X (2004). *Inside the SPAM Cartel*. Rockland, Massachusetts: Synergies Publishing.

Taylor, H. (2003, 10 December). Spam Keeps on Growing. Retrieved 31 May 2006, from http://www.harrisinteractive.com/harris_poll/index.asp?PID=424

Trans Atlantic Consumer Dialogue (TACD) (2003). *Consumer Attitudes Regarding Unsolicited Commercial E-mail (Spam)*.

World Summit of Information Society (2003, December). *Declaration of Principles-Building the Information Society: A Global Challenge in the New Millennium*.

Extension of Victimization in Unsolicited E-mail Messages with Attachments (UEMAs): An Explanation of Seeking and Exposing Process

ABSTRACT

While the growing scale of Internet use brings about great convenient for users, phenomena of unsolicited e-mail pose new threats and challenges. Previous literature was concentrated on general analysis of such messages, leaving many particular respects untouched. This study focuses on the extension of victimization of unsolicited messages e-mail with attachments (UEMAs). Based on the analysis of two samples, one comprised of 501 (sampling done in May 2006), and the other comprised of 490 (sampling done in March 2008), pieces of UEMAs, the study finds that e-mail account exposing and seeking can both contribute to victimization; while receiving of unsolicited messages is the initial victimization, reading and reacting to messages could lead to additional victimization from virus attack or financial fraud, and from conspiracy in illegitimate operations such as tax evasion or transaction of falsified documents.

Keywords: E-Commerce, Survey, Cybercrime, Unsolicited E-mail Messages with Attachments (UEMAs), Victimization, Conspiracy

Hacking all the way into spam

The twentieth century witnessed many outstanding creations of human beings, of which the Internet is one extending its power to today. Radical group (2005) found that more than 683 million users held 1.2 billion e-mail accounts in communication and marketing. It implied that, besides other things, each user could have more than one account. In practice, many frequent users have two or more accounts. Despite the convenience that this unprecedented tool creates, unsolicited e-mail message, its by-product, becomes a nuisance that each user meets by chance. Recipients' property rights, fair trade, public morals, cybersecurity, data protection, as well as other content-related and goods-related transgresses and offences all pose great challenges and threats to society that is symbolized by cyberspace (Li 2006).

Many people have no interest in talking about this issue. Even some economists, whom I had conversation with in a conference in 2005, ignored the significance of such a research. Their straightforward logic was that “unsolicited e-mail is everyday phenomena; everyone knows something about it; and no one thinks it so serious.” One of the economists told me that he received spams everyday and deleted them in a few seconds without extra trouble. They tended to devalue the academic subject by ignoring the impact of the research object through raising examples in their own life, which seemed to be strong enough proof and sound enough understanding.

However, numerous authors have scrutinized the phenomenology of unsolicited commercial e-mail (UCE, or unsolicited business e-mail, UBE, or simply spam) from points of view of economics, commerce, law, technology, sociology, culture, and so on. Others have principally dealt with costs and benefits of senders and recipients derived from unsolicited e-mails (Khong 2001, and 2004), general impact on productivity of individual employees and enterprises (Nucleus 2003, 2004), scale and volume of unsolicited e-mails (Radical Group 2005), impact on consumers’ attitudes and confidence towards e-commerce (TACD 2003; Fallows 2003; Harris Interactive 2003), higher possibility of receiving unsolicited e-mail due to online-published addresses (Federal Trade Commission 2002b), ignorance of removal requests by senders (Federal Trade Commission 2002a), and technical and legal solution on unsolicited e-mail (Sorkin 2001).

Few studies, nevertheless, have touched on unsolicited e-mail messages that have attachments, particularly on what kind of risks a single e-mail user might face. Li (2007) was the first known study specifically on such a phenomenon, based on a sample of 501 attachments (sampling done in May 2006). In this study, two samples were used, one is the same sample used in Li (2007), and the other is comprised of 490 pieces (sampling done in March 2008), of unsolicited e-mail messages with attachment, presenting the first analysis of types and validity of sender column, types and validity of subject column, types of offers of message content, and types, sizes and nature of attachments of these messages. In this paper, the term “spam” is deliberately taking into account the lack of a universally-accepted unified definition. At the same time, the author prefers the phrase of “unsolicited e-mail” without the

modifier “commercial” or “business”, in order to enlarge the coverage of UEMAs to virus spreaders in this study.

Literature review

At the same time as the augmented capacity of computers and networks to process information, “a wealth of information” could result in a “poverty of attention” (Simon 1982). Unsolicited business e-mail (UBE) or unsolicited commercial e-mail (UCE) incarnates an instance where e-mail users have to deal with redundant information they anticipate not to consume. Unsolicited e-mail gives rise to an unconstructive representation of e-marketing, alarming e-mail users from trusting e-mail communication.

Unsolicited e-mail sent out to multiple recipients has extensive unfavourable consequences on e-mail marketing. Karnell (2002) found that an increasing number of e-mails had never been read by recipients, and users prefer limiting or disrupting business contacts with these senders. The prevailingness of unsolicited messages exhibited an emergent intimidation to the information society (World Summit on the Information Society 2003, paragraph 37).

Spammer-X (2004) narrated his/her anecdote with reference to reasons and methods of spamming, revealing the astuteness of defeating anti-spam techniques, avoiding being identified, in addition to escaping the law. McWilliams (2005) accounted the world of spammers and spam-fighters, furnishing information on mechanisms of spamming and spam-fighting. Goodman (2004) presented the most typical spam traps and explained why existing solutions were ineffective. Lambert (2003) analysed a wide range of e-mails in attempt to generate a silhouette of spam and develop a profile of spammer.

The United States Federal Trade Commission (1998) speculated the issue from the standpoint of consumer protection, identifying a dozen of most likely spam scams, covering spam and scams from business opportunities, quick money, working at home, to guaranteed loans, and so on.

Li (2006) recapitulated six challenges that the spam brought to society: recipients’ property rights, fair trade, public morals, cybersecurity, data protection, as well as other

content-related and goods-related transgresses and offences. From the standpoint of senders, all these challenges could be classified into two bigger categories: victim seeking and conspirator seeking. From the standpoint of recipients, they were confronted with preliminary victimization (being spammed), supplementary victimization (being defrauded, or attacked by viruses), or committing offences (tax evasion, or transaction and use of falsified documents).

Nucleus (2003) reported in-depth interviews with 117 employees and extensive interviews with 28 IT administrators. They found that an average of 13.3 unsolicited messages reached the employee per day; each employee has to waste an average of 6.5 minutes per day dealing with unsolicited messages. They calculated that unsolicited messages caused an average 1.4 percent of productivity loss per employee per year, tantamount to an average cost of 874 dollars per employee per year.

Nucleus (2004) reported further interviews with employees at 82 Fortune 500 companies. They found that users received an average of twice the number of previous year's unsolicited messages, with an average 3.1 percent of productivity loss in 2004. They also established that the function of technical solution to unsolicited messages became less efficacious.

Fallows (2003) reported the Pew Internet & American Life Project, which collected data from a national telephone survey of 2,200 adults and a compilation of more than 4,000 first-person narratives about unsolicited messages. Their findings showed that unsolicited messages caused some e-mail users to use e-mail less, and trusted the online environment less, while fear of unsolicited messages increased.

The deteriorated consumers' confidence on unsolicited e-mails results from the losing control over their own accounts. Federal Trade Commission (2002a) tested 215 addresses from spam with "remove me" claims, and found that unsubscribe demand was usually ignored. While senders of unsolicited e-mails do not provide effectual unsubscribe method, they are harvesting addresses from all over the Internet.

Federal Trade Commission (2002b) put 250 new, undercover e-mail addresses in 175 different locations on the Internet, including web pages, newsgroups, chat rooms, message boards, and online directions for web pages, instant message users,

domain names, resumes, and dating services. They found that web pages, newsgroups, and chat rooms were all attractive to unsolicited message senders. Federal Trade Commission (2005) found that spammers continued to harvest email address posted on web sites, and to a much lesser extent, those posted on blogs and USENET groups. Masking email addresses when posting on web sites could substantially reduce the risk of harvesting.

Federal Trade Commission (2003a) reported that 66 percent of spam messages were fraudulent in sender or subject columns, or in the message itself. False advertisements might distort the normal market of goods and services, harm the normal trade order, and reduce the consumers' confidence (The Directorate General of Telecommunications Ministry of Transportation and Communications 2005, pp. 6-7). Large volume of spams, malicious programs and malicious linkages contained in messages were main threats (PC World 2003).

Harris Interactive surveyed 2,376 adults online in 2003, and found that most online adults reported that they had received more spam than six months earlier. Only 14 percent have seen a decline in the volume of spam. A majority of respondents reported unsolicited messages annoying or very annoying (Taylor 2003).

Many spammers send messages by unauthorized use of accounts of other individuals or organizations (Organization of Economic Cooperation and Development 2004). E-mail addresses harvesting software can collect this information automatically from web pages (Boldt, Carlsson and Jacobsson 2004, p. 8). Based on discussion of spyware and findings from two experiments, Boldt, Carlsson and Jacobsson (2004, p. 4) concluded that spyware had a negative effect on computer security and user privacy. Spyware enables spreading of e-mail addresses that may result in receiving unsolicited e-mails.

Khong (2004) stated that although it was difficult to measure costs and benefits of the spammer, if the benefit obtained from the activity outweighs the cost, the spammer would carry out spamming activity. It follows that if there is one successful commercial transaction, the spammer can realize his or her benefit. The costs that are involved in the spamming can be roughly estimated according to costs of bandwidth, message sending, and obtaining of users' address. Costs of bandwidth and message sending are ignorable. According to Sadowsky

(2003, p. 55), the spammer could obtain users' e-mail address in 13 situations. Obviously, the most convenient and least expensive way is to harvest e-mail addresses automatically with specific software, which is also available from Internet, either being free of charge or with an inexpensive price.

The revenue of spammer from sending message has been found high in a few studies (Goodman and Routhwaite 2004). Cobb (2003, p. 2) suggested the concept of "the parasitic economics of spam," meaning that the act of sending a message cost the sender less than it cost all other parties impacted by sending of the message.

Costs and benefits of the spammed can also be estimated. Costs induced by spam to the spammed have a wide coverage, including waste of users' time, bandwidth and storage, cost of anti-spam solution, and cost of overloading at the mailbox (Gauthronet and Drouard 2001). The average time and money lost in processing a single message might not be so significant. However, theoretically, aggregate losses of time and money taken in dealing with these messages might be huge (Li 2006). Spam also induces costs of bandwidth and storage, losses in interruption of services, and anti-spam solutions (Gauthronet and Drouard 2001). Interruption of services is unfortunate for both providers and users in causing business, confidence, and other losses. Worldwide revenue for anti-spam solutions will exceed 1.7 billion dollars in 2008 (IDC 2005). If e-mail address has ever been put on institution's Web site, or personal homepage, it is highly possibly that the address will be harvested, sold, and abused by senders (Federal Trade Commission 2003b).

Finally, unsolicited e-mail is nothing useful and beneficial to recipients. From all of the previous studies, it is reasonable to conclude that recipients undertake pure losses, not only the monetary, but also the psychological (Li 2006).

Methodology

The paper presents a case study on UEMAs, analysing the sender column, subject column, content and attachments of these message. Two samples were used, one was composed of 501 messages, and the other was composed of 490 messages, with attachments out of total approximately 78,820 unsolicited e-mail messages received in an e-mail account

during June 2005 to March 2008. When the sample was taken, UEMAs constituted 19.2 % of all the 26,160 unsolicited e-mail messages. When the second sample was taken, they constituted 9.3 % of 56,750 unsolicited e-mail messages collected during the same period. Figure 1 gives a snapshot of the e-mail account, showing the quantity of messages.

The account has received 78,910 messages in total, with normal messages accounting for a small proportion20and 78,820nsolicited messages in folders “research “research1, “501and “490. 501 UEMAs have been collected in folder “510.The 490 UEMAs have been collected in folder “490.” The first sample, which constituted the framework of this study, was analyzed in May 2006. The second sample, analyzed in March 2008, was primarily used to supplement the previous findings.



Figure 1 Snapshot of the e-mail account showing the quantity of messages (as of 30 March 2008)

Because of the private nature of this e-mail account, it is easy to judge which message is unsolicited. In analysing each message, it is necessary to establish a standard to categorise messages into different types according to their sender column, subject column, content and attachments. The standard to decide if the sender column is falsified is the name format. The name for an organization is also easy to judge by comparing the name in the sender column with that in the content.

The standard for deciding whether a subject column is falsified can be loosely defined. Because there is only one message labelled with an “AD:” sign, in strict sense all the subject columns of other messages are illegal. However, the emphasis of this paper is not to coincide with the legal standard. Rather, it is focused on analysis of phenomena of UEMAs. The message with “AD:” label and messages with words explaining the content or having apparent connection with the content are regarded as not falsified. Other messages with subject column irrelevant with the content, inducing recipient to open messages, is considered falsified. The content is categorised according to offers provided, and the nature of attachments. Analysis of both samples is presented in this paper. Sections about validity of sender column, subject column and content of UEMAs are primarily based on the first sample.

Limits of this study are that the resource account was not broadly put on the Internet, but was published on only one website specialised on traditional publishing service, to soliciting submission of academic articles. It is difficult to determine whether a random sample of all UEMAs sent in the stream of commerce would yield similar findings. It is also unknown that whether publishing- and printing-related UEMAs are due to the resource specialisation.

Findings

Types of File Formats of Attachments

In the first sample of 501 UEMAs, three attachments were missing. Other attachments were comprised of 14 kinds of document formats. More than one third of attachments were “zip” format compressed files, mostly viruses, which represented the most severe threats to the e-mail users’ computer security. Another one third of all attachments were comprised of two categories: approximately one fifth of the total attachments being “gif” format image files, and approximately one sixth being “htm” format documents. This one third was relatively virus free, but included annoying contents and hyper links. These three kinds of files constituted more than 70 percent of all attachments. Another frequent attachment format was Microsoft Word “doc”, which accounted for 8.4 percent of all attachments. Other 10 kinds of document formats were only responsible for approximately 20 percent of

attachments, including both viruses and virus free files.

Three of the second sample of 490 UEMAs lost their attachments. Other 487 messages had 496 attachments, which included more types of files than in the first sample. Text files and “gif” files accounted for nearly 70 percent of these attachments. The most obvious change happened in growing role of text files and declining role of “zip” files, from which I observed that the use of UEMAs had become more rational in advertising practical information other than in spreading viruses. This conclusion was also supported by the decrease of executable files or their disguised formats, such as “com,” “exe,” “pif,” “scr,” and so on. Another observable change was that “html” files decreased by nice percent in attachments. In both samples, “gif” files had a significant percentage, but in fact, they were usually small, benign and meaningless. In sum, types of attachments took on a diversified outlook, with files of familiar formats changing to rational advertisements, and malicious motives seeking unfamiliar formats, at a satisfactorily smaller overall scale.

Table 1 Types of File Formats of Attachments

(In second sample, some messages had multiple attachments)

	Types of File Formats	Attachments in first sample		Attachments in second sample		Change of types Percentage
		Number	Percentage	Number	Percentage	
1	*.chm	11	2.2	4	0.8	-1.4
2	*.com	9	1.8	2	0.4	-1.4
3	*.doc	42	8.4	40	8.1	-0.3
4	*.exe	13	2.6	5	1.0	-1.6
5	*.gif	92	18.5	129	26	+7.5
6	*.htm	78	15.7	32	6.5	-9.2
7	*.jpg	13	2.6	12	2.4	-0.2
8	*.mid	3	0.6	0	0	-0.6
9	*.pif	19	3.8	1	0.2	-3.6
10	*.rar	11	2.2	16	3.2	+1.0
11	*.scr	12	2.4	4	0.8	-1.6
12	*.txt	8	1.6	216	43.5	+41.9
13	*.xls	3	0.6	2	0.4	-0.2
14	*.zip	184	36.9	12	2.4	-34.5
15	*.epf	0	0	1	0.2	+0.2
16	*.hqx	0	0	10	2.0	+2.0
17	*.ini	0	0	1	0.2	+0.2
18	*.pdf	0	0	1	0.2	+0.2
19	*.png	0	0	1	0.2	+0.2

20	*.rtf	0	0	2	0.4	+0.4
21	*.url	0	0	2	0.4	+0.4
22	*.uu	0	0	3	0.6	+0.6
	Mess ages with missi ng attach ment	3		3		
	Total attach ments	498	100	496	100	

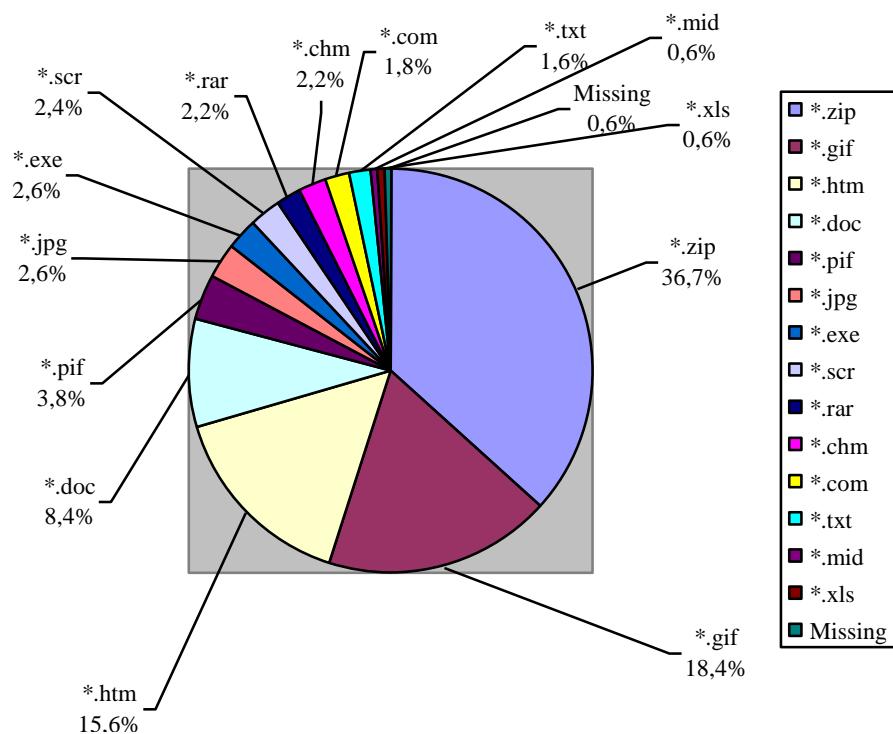


Figure 1 Types of File Formats of Attachments in 2006 Sample

Sizes of UEMAs

The average size of messages in the first sample was 47.44kb. Sizes of approximately 90 percent of UEMAs were smaller than 100kb. Sizes of only 2 percent of these messages were between 100-200kb. Sizes of nearly 9 percent of messages were bigger than 200kb. In fact, about 285 pieces of messages, which constituted more than half of UEMAs, were smaller than 30kb. Messages with the sizes of 1kb and 2kb alone accounted for more than 28 percent of the sample. They were mostly empty “zip” files with the possibility of being UEMAs of viruses

but disinfected by e-mail service providers. UEMAs spreading W32.netsky.C@mm (35k) and W32.Sober.X@mm (75) viruses accounted for 16 percent and 7 percent of all of messages respectively.

In the second sample, the average size was 76.53kb, about 61 percent bigger than that of the first sample. UEMAs smaller than 100kb constituted almost the same percentage as in the first sample. About three percent more messages were between 100 and 200kb, and fewer messages were bigger than 200kb. Nearly 70 percent of messages are smaller than 30kb. UEMAs smaller than 1kb and 2 kb apparently decreased in the second sample, accounting for only 6 percent.

Table 2 Sizes of UEMAs

Size	Massages in the first sample		Massages in the second sample	
	Numbers	Percentage	Numbers	Percentage
<100kb	446	89.0	424	86.5
100-200kb	11	2.2	26	5.3
>200kb	44	8.8	40	8.2
Total size	23,765kb		37,500kb	
Average size	47.44kb		76.53kb	
Among which				
<30kb	285	56.7	377	76.9
1kb	13	2.6	3	0.6
2kb	108	21.6	25	5.1
35kb	80 (Virus: W32.Netsky.C @mm)	16		
75kb	35 (Virus: W32.Sober.X@ mm)	7		
40-45kb			3 (Viruses: W32.Blackmail. E@mm!enc, W32.Lovgate.R @mm)	0.6

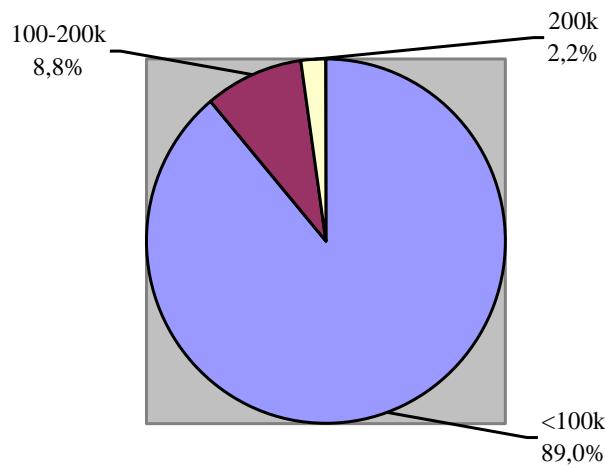


Figure 2 Sizes of UEMAs in 2006 Sample

In the first sample, UEMAs accounted for less than 2 percent of all unsolicited messages. The average size of unsolicited e-mails with attachments was 47.44kb, compared with the average size of 7.32kb of other unsolicited e-mails, a 6.5 fold bigger. In fact, UEMAs contributed to more than 10 percent of the average message size of all unsolicited messages, enlarging the average size from 7.32kb of unsolicited messages without attachments to 8.09kb of all of the unsolicited messages. When calculating message sizes in the second sample, I found that the average size had significantly enlarged, since there were 8 messages with the size ranging from 1mb to 4mb. These messages alone contributed to an average of 31.8kb for all the messages in the sample. Interestingly, large-sized messages were usually sent by political-oriented groups with the intent to spread political speeches.

Table 3 Compare of Average Sizes of Messages in 2006 Sample

	Total size	Numbers	Average size
Average size of unsolicited e-mails with attachments	23,765k	501	47.44k
Average size of other unsolicited e-mails	186,254k	25,459	7.32k
Average size of all unsolicited e-mails	210,019k	25,960	8.09k

Types of Sender Columns in UEMAs

Among the 501 pieces of UEMAs, one is with a blank sender column. Senders of UEMAs tend to hide their names but show e-mail addresses, valid or false. Approximately 60 percent of all messages show e-mail addresses instead of senders' name, which should be considered substandard. Others conceal their names with their surnames and titles, meaningless letters and numbers, describing their offers (products, services and activities), filled with words inducing users to open messages, or simply exploiting recipients' names and e-mail address. In total, approximately 83 percent of messages bear substandard sender columns. Only around one sixth of messages bear standard personal names or company names.

Table 4 Types of Sender Columns in UEMAs

Types of sender columns	First sample		Second sample		Changes in percentage
	Number	Percentage	Number	Percentage	
Blank	1	0.2	1	0.2	0
Company name	45	0.9	27	5.5	+4.6
Describing products, services and activities	16	3.2	136	27.8	+24.6
Inducing users to open messages	7	1.4	14	2.9	+1.5
Meaningless letters and numbers	23	4.6	105	21.4	+16.8
Recipients' name and address	4	0.8	1	0.2	-0.6
Showing e-mail address	297	59.3	72	14.7	-44.6
Standard personal name	79	15.8	86	17.6	+1.8
Surname plus title	29	5.8	48	9.8	+4.0
Total	501	100	490	100	

In the second sample, messages with sender columns describing products, services and activities increased by a quarter. Messages with sender columns comprised of meaningless letters and numbers increased by nearly 17 percent. Showing e-mail addresses in sender columns decreased nearly 47 percent.

Valid Sender Columns in UEMAs

With the first sample, I analyzed in more details validity of sender column, subject column, and content. The following sections are primarily based on the first sample. Senders of UEMAs that were currently empty, or with the content of offering banking or financial services, sales of falsified certificate, human resources recruitment, publishing and printing, sales of health products and clothes, soliciting friends, and with the purpose of merely spreading computer viruses were reluctant to provide sender names in standard formats. Senders of UEMAs who offered telecommunications services were also quite reluctant to do so. Approximately one in every three senders of UEMAs offering information on companies and websites, sales of books, VCD and DVD provided valid name format in sender column. Half of quick money opportunities providers typed right names in their messages' sender column. Senders of UEMAs that offered tax evasion assistance seemed more active in providing standard format of names in the sender column. More than half of them did so. Sixty percent of senders who offered information on training and education opportunities typed names in standard format in the sender column. The providers of computer hardware and software appeared the most reliable senders of UEMAs, of whom more than 70 percent furnished standard sender column. One quarter out of senders who offered other services gave valid form of names.

Table 5 Valid Sender Columns in UEMAs in 2006 Sample

Type	Number of validity in sender column	Percentage
Banking, financial	0	0
Empty attachments	0	0
Falsified certificate	0	0
Human resources recruitment	0	0
Introduction of company, website	6	33.3
Political propaganda	14	56
Publishing, printing, card manufacture, etc.	0	0
Quick money	1	50
Sales of books, VCD, DVD	4	36.4
Sales of health products, clothes	0	0
Software, computer products	33	70.2
Soliciting friends	0	0
Tax evasion	37	53.6
Telecommunications services	1	3.4

Training and education	6	60
Virus	0	0
Other services	1	25

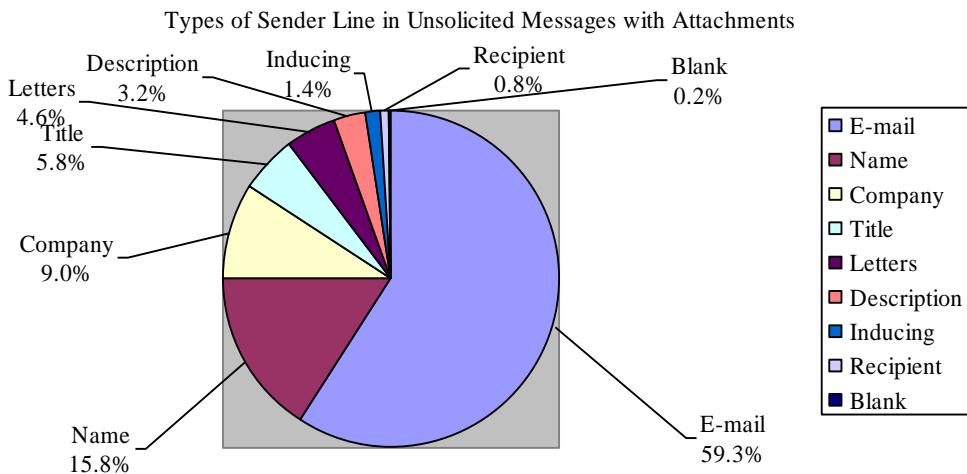


Figure 3 Types of Sender Columns in UEMAs in 2006 Sample

Types of Subject Columns in UEMAs

To label the subject column with “AD:”, “ADV:”, or any other kinds of regulatory means, was an invention that had never been respected by senders of unsolicited messages. According to calculation of the first sample, only less than two in one thousand messages had this kind of label. Two in one hundred of UEMAs left the subject column blank. More than 17 percent of messages used ambiguous wording to confuse recipients, or other particular terms attempting to draw recipients’ attention and attracting them to open messages, furnished the subject column with languages describing the content, giving greetings, appearing related to users’ e-mail service, bearing “To:”, “Re:” and “Fw:” labels, or pretending users’ friends and contacts, etc. The hacking tactics of so-called social engineering was to a great extent used in these messages. In the second sample, messages with subject columns describing message content increased by nearly 50 percent, while messages with subject columns pretending to be recipient’s contact decreased by more than 40 percent.

Table 6 Types of Subject Columns in UEMAs

	First	Second	Change in

	sample		sample		percentage
Type	Number	Percentage	Number	Percentage	
“AD:” label	1	0.2	0	0	-0.2
Attractive wording	87	17.4	26	5.3	-12.1
Blank	10	2	8	1.6	-0.4
Describing message content	117	23.4	354	72.2	+48.8
“To:”, “Re:” and “Fw:” label	21	4.2	25	5.12	+0.92
Users’ friends and contacts	265	52.9	44	8.98	-43.92
Other	0	0	33	6.7	+6.7
Total	501	100	490	100	

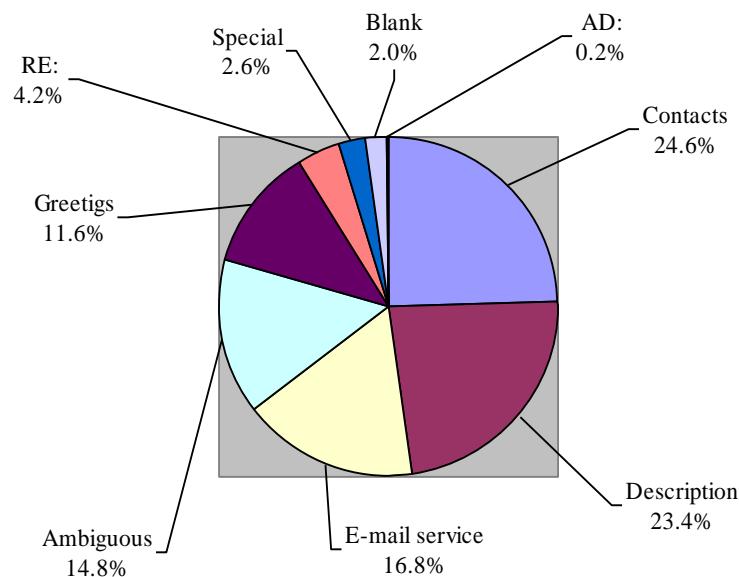


Figure 4 Types of Subject Column in UEMAs in 2006 sample

Valid Subject Columns in UEMAs

Almost all of senders of UEMAs offering information on human resources recruitment, companies or websites, publishing, printing, card manufacture, etc., sales of health products, clothes, and tax evasion ensured the valid subject column. A high percentage of providers of telecommunications services, sellers of books, VCDs, and DVDs, training information providers, quick money information providers, and providers of other services provided valid subject columns in their messages. All senders of other messages were reluctant in typing

useful subjects for their potential recipients.

Table 7 Valid Subject Columns in UEMAs in 2006 Sample

Type	Number	Percentage
Bank, financial	0	0
Empty attachments	11	10.7
Falsified certificate	0	0
Human resources recruitment	2	100
Introduction of company, website	18	100
Political	1	4
Publishing, printing, card manufacture, etc.	19	100
Quick money	1	50
Sales of books, VCD, DVD	8	72.7
Sales of health products, clothes	4	100
Software, computer products	1	2
Soliciting friends	0	0
Tax evasion	66	95.6
Telecommunications services	24	82.8
Training	7	70
Virus	0	0
Other services	3	75

Types of Content of UEMAs

More than 28 percent of messages were designed to spread viruses. More than one in five messages attached empty attachments. Messages offering both tax evasion services and software and computer products constituted around 10 percent of all messages. Any of contents of other messages constituted a percentage far below 10 percent, with messages offering telecommunications services and political propaganda constituting around 5 percent separately. Interestingly, there was rarely any message with attachment involving adult contents, investment chances, sales of pirated software, and some other common offers in messages without attachments.

Table 8 Types of Content of UEMAs in 2006 Sample

Type	Number	Percentage

Bank, financial	3	0.6
Empty attachments	103	20.6
Falsified certificate	10	2
Human resources recruitment	2	0.4
Introduction of company, website	18	3.6
Political	25	5
Publishing, printing, card manufacture, etc.	19	3.8
Quick money	2	0.4
Sales of books, VCD, DVD	11	2
Sales of health products, clothes	4	0.8
Software, computer products	47	9.4
Soliciting friends	4	0.8
Tax evasion	69	13.8
Telecommunications services	29	5.8
Training	10	2
Virus	141	28.1
Other services	4	0.8

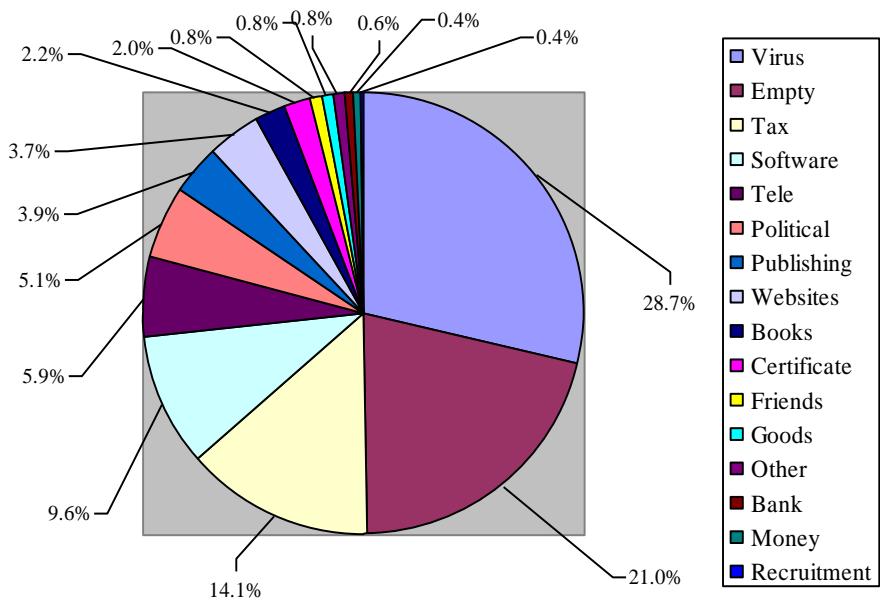


Figure 5 Types of Content of UEMAs in 2006 Sample

Valid Content in UEMAs

Interestingly, most messages had high percentage of valid contents, with exception of messages with empty attachments and UEMAs that spread viruses.

Table 9 Valid Content in UEMAs in 2006 Sample

Type	Number of validity in content	Percentage
Bank, financial	0	0
Empty attachments	0	0
Falsified certificate	9	90
Human resources recruitment	2	100
Introduction of company, website	13	72
Political	25	100
Publishing, printing, card manufacture, etc.	19	100
Quick money	1	50
Sales of books, VCD, DVD	11	100
Sales of health products, clothes	4	100
Soliciting friends	4	100
Software, computer products	47	100
Telecommunications services	24	82.8
Training	8	80
Virus	0	0
Other services	1	25

Types of Contact Methods Provided in UEMAs

Because many UEMAs were spreading viruses, they generally provided no contact information, with a few exceptions. Other messages included one or more kinds of contact methods in the message texts. Of total 501 messages in the first sample, more than one-third of messages provided hyperlinks directed to websites, while less than one-third provided fixed telephone numbers. Both e-mail addresses and mobile phone numbers were preferred by

more than 22 percent of senders. Fax numbers and physical addresses were included in about 16 and 10 percent of messages separately. QQ (a chat system) were provided in 8 percent of messages. MSN was the least used contact method in the 501 messages.

Unsubscribe is nothing more than a decoration in UEMAs. Unsubscribe method was only provided in 2.2 percent of messages in the first sample.

Table 10 Types of Contact Methods Provided in UEMAs in 2006 Sample

Contact Methods	Number	Percentage (/501)
Address	50	10
E-mail	113	22.6
Fax	79	15.8
MSN	12	2.4
Mobile phone	112	22.4
QQ	40	8
Telephone	145	28.9
Unsubscribe method	11	2.2
Website	182	36.3

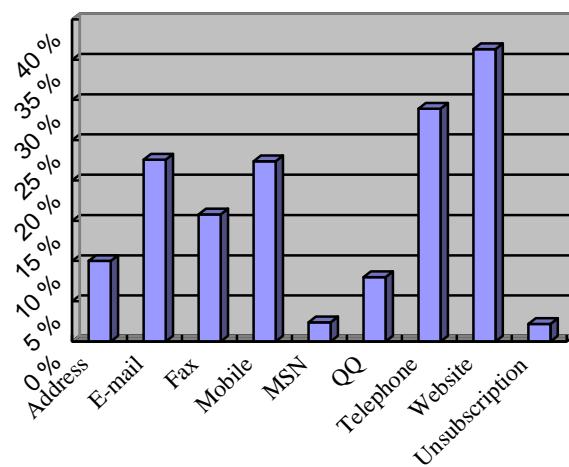


Figure 6 Types of Contact Methods Provided in UEMAs in 2006 Sample

Falsity of Sender, Subject and Content

In the first sample, only one in five of UEMAs used valid format in sender column, one in three used valid subject column, and more than half provided valid content. However, only 58 messages had both valid format of sender and subject column, and 293 messages with both

false format of sender and subject column. Other 42 messages had valid format of sender column but false format of subject column, while 108 messages had false format of sender column but valid format of subject column. The overall falsity of subject or sender column constituted 88.4 percent.

Table 11 Validity and Falsity of Sender and Subject Columns and Content Separately

		Number	Percentage
Sender	Valid	100	20
	False	401	80
Subject	Valid	166	33.1
	False	335	66.9
Content	Valid	260	51.9
	False	241	48.1

The validity and falsity of content took almost 50 percent separately.

Table 12 Validity and Falsity of Either Subject or Sender Columns

		Sender		
		Valid	False	Total numbers
Subject	Valid	58	108	166
	False	42	293	335
	Total numbers	100	401	501
	Percentage	20	80	100
	Percentage of validity of both columns	11.6		

Discussion

In activities of sending unsolicited e-mail messages, one of the most important aspects is to induce recipients to open and read messages and their attachments. Senders of UEMAs took particular considerations in disguising their real identity and real purpose. It can be said that most of them demonstrated a high degree of skill in motivating recipients to open messages and their attachments. However, opening messages and attachments was usually the first step towards for senders to victimize other users. Generally, they used ambiguous wording in sender and subject columns but valid content (except messages spreading viruses)

so as to ensure messages and attachments be open and advertisements be read.

Analysis of the two samples roved that, except messages deliberately spreading viruses, UEMAs were usually less harmful than it was found in findings of previous studies that did not distinguish UEMAs from those without. It implied that senders of unsolicited e-mail messages tended to transform their product or service information.

At the same time, this study revealed that UEMAs could have broader negative impact on criminal phenomena, not only victimization, but also conspiracy. E-mail communications could be taken as an offensive means by which recipients were victimized, or a conspiracy tool with which recipients were seduced to commit crimes. UEMAs that spread viruses could directly result in victimization of recipients, their computers damaged or manipulated, or their secret or privacy stolen or disclosed. Some UEMAs could move recipients to invest their money to projects that could never generate any reward. Some UEMAs could victimize recipients in crimes that recipients being physically or sexually attacked. Or, these messages could induce recipients to collaborate on some criminal plots.

In cyber environment, the most frequent victimization model began from exposing of victims to potential threats, which we can label as exposing-victimization model. Under this model, the victim of UEMAs exposed their addresses merely on web pages, in bulletin board systems (BBSes), in chat systems, or simply in transmission through the Internet. Exposure on the Internet does not necessarily mean show-off. Rather, it should have been a usual kind of digital presence. Nevertheless, the exposing-victimization model at least implies that senders of UEMAs could easily harvest e-mail addresses in the same way as normal Internet users do

In other cases, senders of UEMAs had a seeking process, and followed the seeking-victimization model. Due to the large quantity of web pages and other Internet-related contents, direct artificial collection of multiple e-mail addresses became inefficient. By making use of specialized software to harvest e-mail addresses from the Internet, senders could collect millions of addresses automatically in a short time. By doing so, they created the seeking-victimization model in sending UEMAs. Besides harvesting, they also exploited dictionary attack and/or automatic alphabetical permutation and combination to enumerate possible usernames in e-mail accounts. All of these methods could be used in seeking process. For senders, an e-mail account with a random word might not represent a specified person;

but for the recipient, he/she would readily be the potential victim of this UEMA.

Victimization of recipients of UEMAs could happen without recipients accessing their e-mail accounts. Their victimization resulted from their e-mail accounts being spammed, whether they accessed their accounts or not. Under current legal framework, receiving of unsolicited messages is sufficient to be regarded as victimization caused by acts that imposed punishment by law.

However, victimization of UEMAs does not end at the initial victimization. The above-mentioned models could be called as the first level effects of UEMAs. The second level effects could take place on basis of the initial victimization. There could also be two sub-models: victimization-victimization sub-model and victimization-conspiracy sub-model.

The victimization-victimization model happened when messages spread viruses, fraudulent sales of goods, or falsified financing and banking services. The first level victimization was for recipients to be spammed, while the second level victimization was for recipients to be attacked or swindled upon opening the malicious programs or following the fraudulent scams.

The second level victimization would not always be accomplished so straightforwardly. Usually involved was a victimization-exposing-seeking-victimization process. The most typical scam of this kind was Nigerian fraud (or 419 fraud), in which recipients of unsolicited messages were firstly victimized by receiving this kind of messages (being spammed). If they made a positive reaction to messages, they were further exposing their vulnerabilities to senders. Upon receiving reply from recipients, senders would further seek vulnerabilities of recipients and at last obtain their property. The process of seeking and exposing might be a long interaction between senders and recipients, who exchanged messages until the final transaction. If senders succeeded in obtaining recipients' property, the last victimization would take place and the scam would come to an end.

The victimization-conspiracy model happened when messages included assistance for tax evasion services, sales of pirated software, sales of falsified documents, and so on. Recipients of such offer were firstly victimized by unsolicited messages; and if they participated in illegal operations, they would become conspirators of senders.

Because recipients of unsolicited messages inducing conspiracy in an illegal operation

would expect to have the luck to benefit from collaborating with senders who pretended to have the potential to give charity, senders were more likely to send this kind of messages. In fact, in Nigerian fraud, senders were usually personating politicians who want to transfer property (money, diamond, and so on) to bank accounts of recipients by claiming to give a significant reward. As a result, recipients, who wished they could have been “conspirators” in a great operation of money laundering, would finally be victimized in scams that they lost advance fees.

Conclusion

Phenomena of UEMAs further proved the low controllability or uncontrollability of cyber environment. Exposed e-mail addresses are vulnerable to unsolicited messages. Unexposed e-mail addresses can be as vulnerable as exposed ones, because address harvesting software can collect potential addresses from transmission route of the Internet. As far as our study is concerned, this process makes extra sense. For senders, both ways could be seen as a process of seeking vulnerabilities. For recipients, both ways could also be seen as a process of exposing vulnerabilities. However, seeking and exposing process has become more abundant and colourful in cyber environment than pre-Internet times.

Mere browse of web pages is the easiest method to obtain e-mail accounts, but it is less efficient because e-mail addresses are usually scattered in many different pages. This process would be time-consuming if thousands or millions of addresses are to be collected. Senders can also purchase millions of addresses of users with different interests from specific vendors, who have the best method and specialized personnel to harvest addresses from all over the cyberspace, and usually establish their own databases of addresses. With an inexpensive price, buyers can conveniently get a large quantity of addresses. In addition, address harvesting becomes automated and prevalent with the help of specified software. Many people who are interested in doing spamming business can easily master uncomplicated skills and collect millions of addresses with such software, which can be downloaded from the Internet free of charge or with a small payment.

Exposing e-mail addresses on the Internet is literally unavoidable, because the exposure

is in so broad a sense that all the normal use of e-mail services could be seen as an exposing process, including sending and receiving messages; publishing on web pages, chat rooms, and BBs; providing as register information in online services; or exposing nothing but coincidence with a dictionary vocabulary; and so on. In fact, exposing a single e-mail account will not be so risky if there is not such a thing as address harvesting technique, because it is an inefficient way to collect single e-mail account one by one from the Internet. However, we cannot simply ignore such a method because e-mail account vendors could collect and transact addresses in a dynamic process, and collect addresses through a variety of ways to establish their databases. Address harvesting software and dictionary attack undoubtedly intensify the victimization of e-mail account holders.

In general, exposed e-mail accounts might face double risks of being victimized: being collected in process of formally browsing web pages and use of other Internet services; and being harvested during the process of digital transmission or merely guessed by senders through randomly combining letters and numbers. Compared with daily used e-mail accounts without exposing on web pages or other Internet services, published accounts are more likely to be spammed. Therefore, it seems more likely that vendors or senders harvest addresses with automated technique. As a result, double risks of exposed e-mail accounts are in fact unbalanced: the risk of being victimized by collectors and harvesters are far serious than that by guessers.

UEMAs provide e-mail users many different choices, either conspiring in criminal acts, or victimized by viruses or in scams. Messages analyzed in this study generally gave recipients two alternatives: conspiring in tax evasion, or damaged by viruses.

In the case of conspiracy in tax evasion, senders used to provide valid contact methods so as to induce recipients to participate in illegitimate operations. The offer seemingly aims to establish a relationship between tax evasion service provider and their potential clients. However, the effect was that they form conspiracy in tax evasion activity. Recipients had to react actively before they become conspirators of tax evasion activities. The process might involve repeated e-mail exchanges upon initial unsolicited messages. Under these circumstances, unsolicited messages might be transformed into literally valuable (but morally wrong and legally prohibited) information for recipients. Thus recipients might tend to accept

such messages and offers in them. Such messages become the communication means for criminals, posing great threats for social control over illegal activities.

In the case of viruses attack, senders exploited social engineering to induce recipients to open messages and their attachments, by blurring sender, subject columns and falsifying message content and file names of attachments. These messages did not require any reply from recipients before they caused damages. They were also dangerous for recipients in the sense that they were harming recipients' hardware and software, wasting time and labour.

References

Boldt, M., Carlsson, B., & Jacobsson, A. (2004). Exploring Spyware Effects. Retrieved April 1, 2008, from <http://www.tml.tkk.fi/Nordsec2004/Presentations/boldt.pdf>

Cobb, S. (2003). The Economics of Spam. Retrieved April 1, 2008, from http://www.spamhelp.org/articles/economics_of_spam.pdf

Fallows, Deborah (2003, October). Spam: How It Is Hurting E-mail and Degrading Life on the Internet. Retrieved April 1, 2008, from http://www.pewinternet.org/pdfs/PIP_spam_Report.pdf

Federal Trade Commission (1998, July). Federal Trade Commission Names Its Dirty Dozens: 12 Scams Most Likely to Arrive via Bulk E-mail, *Federal Trade Commission Consumer Alert*. Retrieved April 1, 2008, from <http://library.findlaw.com/1998/Jul/1/128450.html>

Federal Trade Commission (2002a, April), *Remove Me Surf*, Author. Retrieved April 1, 2008, from <http://www.ftc.gov/bcp/conline/edcams/spam/pubs/removeme.pdf>

Federal Trade Commission (2002b, November), E-mail Address Harvesting: How Spammers Reap What You Sow, Author. Retrieved April 1, 2008, from <http://library.findlaw.com/2003/Aug/8/132973.pdf>

Federal Trade Commission (2003a, April), *False Claims in Spam: A Report by the Federal Trade Commission's Division of Marketing Practices*, Author. Retrieved April 1, 2008, from <http://www.ftc.gov/reports/spam/030429spamreport.pdf>

Federal Trade Commission. (2003b, June 15). *National Do-Not-E-mail Report to Congress*, Author. Retrieved April 1, 2008, from <http://www.ftc.gov/reports/dneregistry/report.pdf>

Gauthronet, S., & Drouard, E. (2001). *Unsolicited Commercial Communications and Data Protection*. Brussels: Commission of the European Communities, Internal Market Directorate General. Retrieved April 1, 2008, from http://ec.europa.eu/justice_home/fsj/privacy/docs/studies/spamsum_en.pdf

Goodman, Danny (2004), Spam Wars: Our Last Best Chance to Defeat Spammers, Scammers & Hackers, New York, New York: SelectBooks.

Goodman, J. T., and Rounthwaite, R. (2004). Stopping Outgoing Spam. In: *Proceedings of the 5th ACM Conference on Electronic Commerce*, 17-24 May, ACM Press, pp. 30-39. Retrieved April 1, 2008, from <http://research.microsoft.com/~joshuago/outgoingspam-final-submit.pdf>

IDC (2005, February 24). Worldwide Revenue for Antispam Solutions To Reach Over \$1.7 Billion in 2008, IDC Reveals. *IDC - Press Release*. Retrieved April 1, 2008, from http://findarticles.com/p/articles/mi_m0EIN/is_2005_Feb_24/ai_n10300118

Karnell, J. (2002). Raising the Stakes in Permission Marketing. Retrieved April 1, 2008, from <http://www.onetooneinteractive.com/resource/whitepapers/0003.html>

Khong, W. K (2001, October). The Law and Economics of Junk E-mails (Spam). Retrieved April 1, 2008, from <http://www.emle.org/Thesis/Khong.pdf>

Khong, W. K. (2004). An Economic Analysis of Spam Law. *Erasmus Law and Economics Review*, 1 (February), 23–45. Retrieved April 1, 2008, from <http://www.eler.org/include/getdoc.php?id=8&article=2&mode=pdf&OJSSID=6170ccc598edb033fc0ccf2477a86ee9>

Lambert, Anselm (2003, September). *Analysis of Spam*. Master of Science in Computer Science Dissertation, Dublin: University of Dublin.

Li, Xingan. (2006). E-marketing, Unsolicited Commercial E-mail, and Legal Solutions, *Webology*, 3(1), Article 23. Retrieved April 1, 2008, from <http://www.webology.ir/2006/v3n1/a23.html>

Li, Xingan (2007). The Phenomenon of Unsolicited E-mails with Attachments. *SIMILE: Studies In Media & Information Literacy Education*, 7 (2), 1–11.

McWilliams, Brian (2005). *Spam Kings*, Sebastopol: O'Reilly Media.

Nucleus (2003). *Spam: The Silent ROI Killer*, Research Note D59. Retrieved April 1, 2008, from <http://www.spamhelp.org/articles/d59.pdf>

Nucleus (2004). *Spam: The Serial ROI Killer*, Research Note E50. Retrieved April 1, 2008, from http://tim.blog.kosmo.com/article_files/NucleusResearchCostOfSpam.pdf

Organization of Economic Cooperation and Development (2003). *Organization of Economic Cooperation and Development Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices Across Borders*, Author. Retrieved April 1, 2008, from http://www.oecd.org/document/56/0,2340,en_2649_34267_2515000_1_1_1_1,00.html

Organization of Economic Cooperation and Development (2004). *Second Organization of Economic Cooperation and Development Workshop on Spam: Report of the Workshop*, Author. Retrieved April 1, 2008, from <http://www.oecd.org/dataoecd/55/32/31450810.pdf>

PC World (2003, August 29). Sobig May Be Working for Spammers. Retrieved April 1, 2008 from <http://www.pcworld.com/news/article/0,aid,112261,00.asp>

Radical Group (2005). *The Radical Group, Inc. Release Q1 2005 Market Numbers Update*, Author. Retrieved April 1, 2008, from http://www.radicati.com/uploaded_files/news/Q1-2005_PressRelease.pdf

Sadowsky, G., Dempsey, J. X., Greenberg, A., Mack, B. J., and Schwartz, A. (2003). *Information Technology Security Handbook*. The International Bank for Reconstruction and Development.

Simon, H. A. (1982). *Designing Organizations for an Information-Rich World: Models of Bounded Rationality*. Massachusetts: Massachusetts Institute of Technology Press.

Sorkin, D. E. (2001). Technical and Legal Approached to Unsolicited Electronic E-mail, *University of San Francisco Law Review*, Vol. 35, pp. 325-384. Retrieved April 1, 2008, from <http://www.sorkin.org/articles/usf.pdf>

Spammer-X (2004), *Inside the SPAM Cartel*, Rockland, Massachusetts: Synergies Publishing.

Taylor, Humphrey (2003, 10 December). Spam Keeps on Growing. Retrieved April 1, 2008, from http://www.harrisinteractive.com/harris_poll/index.asp?PID=424

Trans Atlantic Consumer Dialogue (TACD) (2003). *Consumer Attitudes Regarding Unsolicited Commercial E-mail (Spam)*, Author. Retrieved April 1, 2008, from http://www.tacd.org/db_files/files/files-296-filetag.doc

World Summit of Information Society (2003, December). *Declaration of Principles-Building the Information Society: A Global Challenge in the New Millennium*, Author. Retrieved April 1, 2008, from http://www.itu.int/dms_pub/itu-s/md/03/wsis/doc/S03-WSIS-DOC-0004!!PDF-E.pdf

Federal Trade Commission (2005). Email Address Harvesting and the Effectiveness of Anti-Spam Filters: A Report by the Federal Trade Commission's

Division of Marketing Practices, November 2005, 10 pp. Retrieved April 1, 2008, from <http://www.ftc.gov/opa/2005/11/spamharvest.pdf>

费者权利保护方面，民法调整的是平等主体的商家和消费者的关系，但是《民法通则》在制定时忽略了一点就是平等民事主体之间的关系可能有平等的关系和不平等的关系，很显然，商家在信息力等方面占有了绝对的优势，如果完全按照民法来调整的话显然不利于消费者利益的保护，这种情况下，就必须以国家或社会的力量涉入这一关系中，通过调整国家与商家的关系从而达到双方的平衡。随着生产社会化的发展，民法单纯的个人本位越来越表现出局限性，为适应不断发展的社会现实，民商法开始了现代化的进程，对个人本位做出了一定的修正，通过公序良俗等原则的确立，体现了对社会利益的一定关注。但是民商法的基础仍然是私权神圣、意思自治、契约自由，因而民商法不可能给与社会利益以充分的保护。经济法从产生起就以社会整体利益的实现为其使命，它要求个体和局部利益服从社会整体利益，短期利益服从长远利益。

经济法是由于近代生产社会化的大发展，国家为避免市场机制的缺陷给经济造成的失调而产生的，因此传统的经济法学者对经济法的研究不可避免地集中于如何进行市场监管和宏观调整方面上。当代社会，随着市场经济全球化和高新技术的突破性发展，经济的飞速发展使经济活动由个体经济发展为整体经济。经济活动以家庭、企业、个体利益为重心让位与整体利益为中心并要求从法律上加以确认；经济发展的目标是社会再生产的良性循环。相应地，经济法也空前繁荣，并凸显出自己不可替代的特点，是国家经济发展战略的保障。相应地经济法的基本特征更加明显，即综合调整，公法与私法互相渗透和社会责任本位。与其他部门法相比，经济法对弱势群体保护的视角具有经济性、宏观性，充分体现了经济法的社会本位性，进一步说明经济法的调整对象是特定的经济关系，而不是所有的经济关系；经济法的本质是国家从社会整体利益出发调控社会经济，使之良性运行、协调发展之法。目前在中国的经济转型时期社会性弱势群体的出现与经济体制、经济结构的不完善是分不开的，因此经济法必须尊重各经济主体的经济自由，维护其经济权利，要控制国家调节管理主体的权力，防止滥用。效益与公平是经济法基本价值。经济法要协调个体与社会总体的经济效益和利益，不能偏废；要维护社会各主体间的实质公平。相应地，对弱势群体的保护成为经济法研究中的新亮点。通过以上分析可以看出，经济法的研究范围是非常广泛的，并且随着经济生活的发展，其内容也不断丰富和扩冲，但并不意味着经济法无所不包。我们必须采取谨慎的态度去对待，不能想当然地为其研究领域于其他部门法去争执，以免使经济法处于包罗万象的尴尬境地。

参考文献：

1. 《经济法通论》 中南政法学院经济法系编 经济科学出版社 1986 年
2. 《经济法学评论》 史际春主编 中国法制出版社 2000 年
3. 《社会保障制度改革》 张琪，刘雄主编 经济管理出版社 1996 年
4. 《社会保障学：理念、制度、实践与思辨》 郑功成著 商务印书馆 2000 年
5. 《社会保障法》 覃有土，樊启荣编著 法律出版社 1997 年
6. 《经济法的理论问题》 梁慧星，王利明著 中国政法大学出版社 1986 年

Spam Solutions: A Law and Economics View

Li Xingan*

Li, Xingan (2005), *Spam Solutions: A Law and Economics View*, *Asian and Comparative Law*, Vol. III, No. 1, 2005.

Abstract: The paper begins with a precise description of the phenomenon, and continues in section II to classify the Spam. In Section III, the paper lists the problems brought about by Spam, such as fraud and deception, pornography, security implications and identity theft. Section IV gives a sketch of the scale of Spam. Section V is an analysis of the costs and benefits of sender and recipient of Spam. The paper examines

* Researcher, Faculty of Social Sciences, University of Joensuu, Finland.

effect of the four primary solutions, including technological, market, educational and regulatory in Section VI and VII. Special reference is placed on the economics analysis of different regulatory modes. At last, the paper ends with conclusions that Spam must be eliminated by comprehensive mechanisms.

Key words: direct marketing, Spam, law and economics

JEL Codes: D18, K14, K42, M31

I Introduction

As the increase of capability of computers and the networks to generate, store, and transmit information, "a wealth of information" can lead to a "poverty of attention" (Simon 1982). Pool et al. (1984) demonstrated that the supply of information has been growing faster than people's ability to consume it.

There are about 683 million E-mail users worldwide with nearly 1.2 billion active E-mail accounts in April 2005. These users send and receive 130 billion E-mail messages per day, although two thirds of that is Spam (Radical Group 2005). Forrester (Niall 2000) describes E-mail marketing as one of the most effective online marketing tools, and expects E-mail marketing to be worth \$5 billion by 2004. Peppers and Rodgers (2000, p 4) claim that "clear benefits, including high response rates and low costs are rapidly turning E-mail marketing into an invaluable tool".

However, Spam sent out to multiple recipients, stains the name of E-mail marketing; to avoid being perceived as Spam, authors suggest firms should restrict the messages they send (Wreden 1999; Wright and Boling 2001). Research (IMT Strategies 2001) found a growth in unopened E-mails, and increased action on the part of consumers to limit or remove most commercial online relationships.

Once considered minor nuisance, Spam has proven to be an increasingly large problem. In an Infoworld article (2003), over 40% of respondents listed Spam as the worst IT problem of the previous year. The scale and effect of the Spam prevalence implies that Spam has become "significant and growing problem for users, networks and the Internet as a whole" (WSIS Declaration, paragraph 37)

Most people have some unclear awareness that it came from at first from the "Spam skit by Monty Python's Flying Circus" (Templeton 2003). However, the history of Spam can be traced back to the late 1970's with BBSs, MUDs and MUSHes and USENET groups that were sent multiple mailings by the likes of Canter and Siegel, Rob Noha, and Dave Rhodes. These early mass mailings were not considered Spam at first but subsequently spread wide on the Internet (Templeton 2003). Templeton (2003) cites an example of E-mail Spam sent by DEC in 1978. Kelly (2002) explored the history of Spam and believes that it was born on 12 April, 1994. Spam came to prominence after the Canter and Siegel incident (Kelly 2002).

MAPS (2004) defines Spam as:

"An electronic message is "Spam" if: (1) the recipient's personal identity and context are irrelevant because the message is equally applicable to many other potential recipients; and (2) the recipient has not verifiably granted deliberate, explicit, and still-revocable permission for it to be sent; and (3) the transmission and reception of the message appears to the recipient to give a disproportionate benefit to the sender."

During the Geneva phase of the World Summit on the Information Society (WSIS), Spam was identified as a potential threat to the full utilization of the Internet and e-mail (ITU 2004a).

After giving a precise description of the phenomenon, the paper continues in section II to classify the Spam. In Section III, the paper lists the problems brought about by Spam, such as fraud and deception, pornography, security implications and identity theft. Section IV gives a sketch of the scale of Spam. Section V is an analysis of the costs and benefits of sender and recipient of Spam. The paper examines effect of the four primary solutions, including technological, market, educational and regulatory in Section VI and VII. Special reference is placed on the economics analysis of different regulatory modes. At last, the paper ends with conclusions that Spam must be eliminated by comprehensive mechanisms.

II Classification

Due to the complexity of the phenomenon, Spam can be classified in different ways. The delivery mode of Spam includes through E-mails, newsgroups, mobile phones Short Message Service (SMS) and instant messenger services (Batista 2000). The sender of Spam can be classified as strangers, acquaintances, and subscription services (Hise 1999). The content of Spam can be classified as commercial, political, industrial, chain mails, and others such as self-spreading virus E-mails (Foster 2000).

The US Federal Trade Commission identified twelve most likely Spam scams: business opportunity scams, making money by sending bulk E-mailing, chain letters, work-at-home schemes, health and diet scams, easy money, get something for free, investment opportunities, cable descrambler kits, guaranteed loans or credits on easy terms, credit repair scams, and vacation prize promotions (FTC 1998).

The sender's motive can be classified as informational, disrupting the working of a recipient or E-mail service provider's (ESP) network, and confusing or misinforming the recipients.

Classification of Spam is vital from a legal standpoint, because most Spam legislation targets a particular type, such as business E-mails, or deceptive Spam.

III Problems related to spam

1 Fraud and deception

66% of Spam messages are fraudulent in their “from” or “subject” lines, or in the message itself (FTC 2003b). Spammers disguise the origin of their messages because Spammers know their messages are being blocked or filtered; and aim to entice individuals to open their messages. These kinds of problems include false “from” and “reply-to” addresses, false routing information, deceptive subject lines, and fraudulent removal representations (FTC 2003a). It is also commonplace for Spam to include deceptive or misleading representations in the body of the message, such as the Nigerian scam, those promoting pyramid and bogus no-risk investment schemes, advertising “miracle” diets and health products, credit card or credit improvement offers, attractive travel packages or business opportunities, and messages promoting prostitution, illegal online gambling services, drugs or weapons sales, etc.

2 Pornography

Spam messages containing pornographic photographs, and promoting adult entertainment products and services are not appropriate for children. Since many Spammers do not target specific recipients, young children are likely to be inadvertently exposed to pornographic or offensive messages.

3 Security implications

Spam can clog up computer networks and temporarily paralyzes or even permanently damage personal computers when used to spread computer viruses or worms. Large volumes of Spam can interfere with critical computer infrastructures and endanger public safety.

Some Spam contains destructive viruses and worms. Brightmail (2003) estimated that 90% of viruses are passed through E-mail. 51% of corporations have had a virus disaster, and computer worms have become prevalent and problematic as well. Files such as spyware can be downloaded with the content of E-mail messages. Spammers also exploit security weaknesses inherent in E-mail transfer technology such as open relays and open proxies. According to MessageLabs, more than 60% of the Spam it traps each month is sent via open proxies (PC World 2003). The linkages between Spammers and writers of malicious code seem to be increasing. Other security issues are raised by the use of Spam to attract unsuspecting users to Web pages where spying software is secretly downloaded.

4 Identity theft

Identity theft is threatening e-commerce by corroding consumer trust. Spammers usually use some other business's IP address or conceal their own identity by using stolen or falsely labelled company identities. Individuals and organizations can be victims of identity theft. Many Spammers send their messages by using someone else's account without permission (OECD 2004).

Spyware can gather and transmit information about a user's activity on the Internet and information about E-mail addresses, passwords, and credit-card numbers (Boldt, Carlsson & Jacobsson 2004, p.8).

IV Scale of Spam

The ease of using Spam to offer goods and services increases the volume of Spam. Jupiter Communications foresees a forty-fold increase in Spam between 1999 and 2005, from 40 pieces to 1,600 pieces received per person annually (Marlin 2000).

According to IDC, a typical organization of 1000 people will receive and circulate 2.1 million Spam messages every year (EquiP Technology & CipherTrust 2004). According to MessageLabs, the average global ratio of Spam to desired e-mails was 94.5% in July 2004 (compared to 52.8% in March 2004) (EquiP Technology & CipherTrust 2004). Sophos statistics show that global Spam at the end of 2004 has reached 3 trillion messages, with an estimated cost of USD 131 billion and that volumes have doubled compared to the end of 2003 (EquiP Technology & CipherTrust, 2004).

V Spam -Externalities in cyberspace

Externalities are defined by economists as the situation in which benefits and profits come by imposing cost on others. Externalities arise when two or more parties want to use the same scarce resource for conflicting purposes. Externalities are an inevitable result of common access to the Internet, a system comprised of scarce resources. Indeed, as more and more uses of this resources are discovered, and more and more people enter the commons, it is not at all surprising to find increasingly costly externality problems arising. People want to use this resource to lower their costs of buying or selling goods and services, to transmit and store data, to communicate with friends and colleagues, and for entertainment, but some people also get pleasure from causing harm to others. The net is sufficiently large to support tremendous numbers of activities, but crowding is becoming an increasingly significant problem (Wikipedia 2005).

In the case of spammers the costs to the recipients are much greater than the costs of the sender. Spamming shifts advertising costs from advertisers to both Internet users and ISPs. This cost-shifting may occur through higher subscription fees, or increased costs to ISPs for disk storage space, anti-spam enforcement, consumer complaints, and system delays (Amaditz 1999).

1 The costs and benefits of the sender

Khong (2004) claims that Spammer will undertake a Spamming activity if the expected benefit outweighs the cost. A Spammer only realizes his benefits when there is a successful commercial transaction following the Spam. However, it is difficult to measure the costs and benefits of the Spammer. A few empirical studies reported the average cost and benefit of a single message.

First, the Detroit Free Press reports (Wendland 2002) that Alan Ralsky, a notorious Spammer, charges \$22,000 to send to his entire database of 250 million addresses, or just about .01 cents per message. The New Zealand Herald (Griffin 2003) reports that one Spammer is paid US\$300 per million messages (.03 cents). In a New York Times interview, Spammer Richard Colbert says that he used to charge \$900 for one million Spams: about .1 cents per message. However, Colbert reports that prices have dropped precipitously recently, as low as \$25 per million: .0025 cents per message (Hansell 2003b).

Second, an article in the Hartford Courant (Moran 2002) says that Ronnie Scelson has revenue of \$30,000 to \$40,000 per 80 million messages, for revenue of as much as .05 cents per message, but is willing to Spam for products that bring as little as \$1000 per mailing (presumably also to 80 million people, or as little as .00125 cents). A Wall Street Journal Article says that Howard Carmack earned \$360 for sending 10 million messages, or .0036 cents per message (Grimes 2003).

Computer technology has cut the cost of delivering messages. Relative to the fixed cost of hardware and software, the marginal cost of delivering an electronic mail message is negligible. Hansell finds that the marginal cost of sending a marketing message to 1 million recipients by electronic mail is less than \$2,000, while the same solicitation sent by conventional, bulk-rate postal mail would cost over \$190,000 in postage, not counting paper and printing costs (Hansell 2003b). In the face of these low costs, it is economically rational for individual commercial E-mailers to distribute their messages as widely as possible. Experts estimate that commercial E-mail is profitable if even one recipient in 100,000 makes a purchase (Hansell 2003b).

In sum, the fact that the spam can be sent at very low cost and in a great quantity has attracted direct marketing companies to use Spam e-mails for advertisement.

2 The costs of the recipient

A survey by Gartner Consulting on E-mail users' perception of Spam found that 83% of the more than 13,100 respondents dislike Spam (Gartner Consulting 1999). E-mail users dislike Spam because of additional cost they have to incur in dealing with them. They have to download the Spam, to read through it to determine whether the content is useful and to delete it if it is not useful. The aggregate loss of time and money in aggregate taken in dealing with these messages might be huge. With the growing dependence of users on the Internet and e-mail for communications, the phenomenon of Spam can seriously hamper the development of the digital economy and society by undermining user confidence in online activities.

EquiP Technology & CipherTrust (2004, p.1) found that the average E-mail user receives up to 70 E-mails a day. According to Ferris Group, the average employee spends 30 minutes each day dealing with Spam. (EquiP Technology & CipherTrust 2004, p.2). A December 2004 survey suggested that internet users spend an average of 10 working days per year dealing with spam, and at least some industry analysts estimate that the 2005 cost of spam to business due to lost productivity and additional network maintenance costs will be around \$50 billion for the year (Zeller 2005, p.3).

Associated with Spam, the primary technical costs are the bandwidth and storage that it uses. A report by the European Union estimates the global bandwidth costs of Spam at \$8-10 billion annually (EquiP Technology & CipherTrust 2004, p.2).

The influx of Spam has caused many people and organizations to deploy some form of anti-Spam solution. A European Commission study estimates that the costs associated with these solutions might come up to 10 billion Euro per year worldwide (Gauthronet & Drouard 2001). Another study finds that the longer an E-mail user retains an E-mail account, the more likely he will be spammed (Gartner Consulting 1999, p. 4).

E-mail users also face a second order cost of overloading at the mailbox. Spam degrades E-mail services, fills up users' mailbox with useless information, and decreases the usefulness of the E-mail service.

The impact of Spam on E-mail service providers is tremendous, as each ESP serves many E-mail users. The more Spam there is, the higher will the bandwidth be required. Similarly, a faster and larger capacity server is needed to process the incoming E-mails and Spam. It is not impossible that an ESP's network is forced to the point of a shut down because of Spam (Goodman 2000).

In order to cope with increasing amount of Spam, ESPs have resorted to filtering and blocking Spam on the users' behalf. Even web-based E-mail services, which derives revenue from banner advertisements that appear when a user reads his E-mails, provide Spam filtering services in order to retain users. GartnerConsulting's survey finds that most E-mail users look favorably at an ESP that offers a Spam filtering service as part of its program (Gartner Consulting 1999, p. 10).

However, a survey in 1998 finds that the ISPs' additional cost of hiring Spam-fighters range from a few hundred thousand US dollars to more than a million per year (Dern 1998).

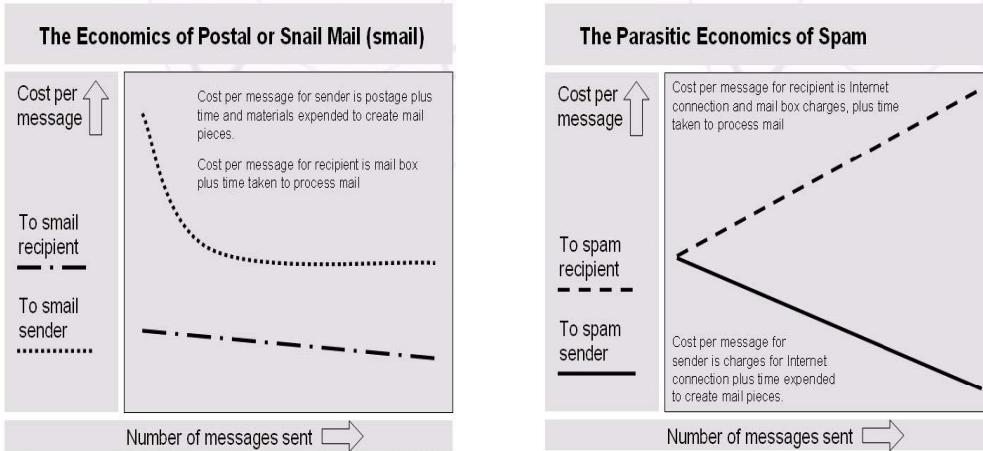
In addition, the third parties bear part of the social cost of Spam. As Spammers usually use a fake E-mail address, and some of the recipient addresses are not valid, bounced messages are relayed back and forth a couple of times between the sender's ESP and the recipient's root server. Bounced Spam further takes up unnecessary network bandwidth. False sender's or reply address poses further problem to third parties. If the reply address belongs to a third party, he will also be unwittingly flamed by angered Spammed recipients.

3 Comparison between traditional mail and E-mail

To better understand the problem of the costs of the senders and the recipients, Cobb (2003) compared the situation between traditional

mail and Spam. He suggested the concept of "the parasitic economics of Spam," meaning that the act of sending a message costs the sender less than it costs all other parties impacted by the sending of the message (Cobb 2003, p.2).

Cobb compared the E-mail with the traditional mail that the postal service delivers and concluded that the cost per message for traditional mail declines as you increase volume, due to printing and handling efficiencies, bulk postage rates, and so on. But after a certain point it stops declining, because there are limits to the sliding scale for bulk mail postage. This can be shown as a curve that flattens out.



Source: Cobb (2003), p.2

Source: Cobb (2003), p. 3

The per message cost of traditional mail to the recipient is low to begin with, and relatively fixed. By contrast, most E-mail users check it multiple times per day, and Spammers are constantly coming up with new ways to make their messages look like legitimate E-mail. This means that sorting is a nontrivial task performed multiple times per day.

On the contrary, per message costs for Spammers start out low and decrease rapidly with volume. In reality, some Spammers pay nothing for sending their messages, hijacking resources that belong to others.

VI Non-legislative solutions to Spam

The popular approaches to managing Spam fall roughly into four categories, technological, market, educational, and regulatory. The first three approaches are analyzed in this section, and the regulatory approach is analyzed in the next section.

1 Technological solutions

Technological solutions to Spam can be divided into two types, i.e. the inbound solution and the outbound solution. Most previous work on Spam has focused on stopping inbound Spam (Dwork & Naor 1993; Naor 1996; Sahami et al 1998; Johanson 2002). Popular approaches include computational approach (Dwork 1993, Johanson 2002), challenge response (including HIPs, Naor 1996; CAPTCHA, Blum et al 2000), rule-based filters (Cranor & LaMacchia 1998), Bayesian filters, and community classification. The best known outbound solution is the adoption of HIP idea (Hansell 2003a).

Unfortunately, no existing solution has been completely effective and most devolve to a technological arms race. Using a single approach tends to result in administrators either "setting the bar too low" and letting in too many unwanted messages, or "setting the bar too high" and blocking legitimate E-mail (Cooley 2004). As long as marginal costs of sending remain low, a Spammer can simply send variation after variation to thwart a filter, eating up bandwidth along the way. When Spam is a negative externality to its recipients, E-mail users will choose to lower their loss of time by filtering mechanisms. Similarly, E-mail service providers may also lower the negative externality by refusing to relay Spam E-mails. Blocking and filtering systems take time and money to install and administer, and they are not without serious and potentially costly side effects of blocking messages in error (Khong 2004).

2 Market solutions

A few articles have explored marketbased mechanisms for allocating receiver attention (Kraut et al 2003; Fahlman 2002; Zandt 2003). Such mechanisms include stamps, surcharges on communication, and auctions. These are promising in that they shift the burden of screening from recipients to senders who know more about message content. One such proposal, focusing on sender surcharges, benefits most recipients and all senders by forcing them to collectively stop overexploiting receiver attention (Zandt 2003). Senders always benefit if either surcharges are rebated to the community, or more accurate recipient profiling allows senders to target more selectively. Shortcomings of focusing on senders include voluntary participation in surcharge mechanisms and also the ability to lie about content ex ante in order to elevate interest.

An experimental investigation of pricing recipient attention via E-mail postage found that charging does cause senders to be more selective and to send fewer messages (Kraut et al 2004). In particular, variable rate usage charges reduced communication more than flat rate access charges.

One well-designed mechanism is outlined by Fahlman in (Fahlman 2002) and more casually in (Ayres & Nalebuff 2003). The main observation is that communications media, such as E-mail, telephone and instant messaging, allow one person to interrupt another and obtain

their attention. Fahlman proposes giving recipients the ability to sell 'interrupt rights' to senders. Strangers must make a binding offer for the privilege of diverting a recipient's attention; they agree to pay an 'interrupt fee'.

3 Education of end users

It is becoming increasingly important that companies recognise the importance of educating end users about Spam and how to recognise and deal with it. A Yahoo survey showing that over 56% of users are unwittingly replying to Spam, the cost in terms of lost hours of productivity is clear. Users must also be made to understand that "friendly fire" also constitutes Spam, and that they should refrain from using company E-mail for these purposes. Furthermore, if users reply to Spam, they often do not realise that this action will probably expose them to a hundred other databases or sources of Spam.

VII Regulatory solutions

1 Opt-in vs. opt-out

1.1 Different legislative models

In regard to how to define the consent of a data subject which is required to obtain to send such Spam e-mails, there are two method, "opt-in" and "opt-out".

The European Union has adopted an "opt-in" approach for commercial communications by E-mail, by way of Directive 2002/58/EC, which is an integral part of the new, wider European Community (EC) regulatory framework on electronic communications.

The Directive contains three basic principles with regard to unsolicited commercial communications. Firstly, according to Art. 13(1) of the Privacy and Electronic Communications Directive member states are required to prohibit the sending of unsolicited commercial communications by fax, E-mail, or other electronic messaging systems such as SMS and Multi-media Messaging Service (MMS) unless the prior consent of the person has been obtained. This regime is applicable for marketing to individuals but member states can extend the scope to marketing communications to businesses. There is a limited exception from the opt-in system for existing customers (Art. 13 (2)) for the use of contact details obtained from customers in the context of a sale, but it may only be used by the same legal person for the marketing of 'similar' products or services and provide an explicit opt-out is offered at the time of collection and with each subsequent message. Secondly, the disguise of identity of the sender is prohibited. Thirdly, direct marketing messages must include a valid return address where persons may opt-out.

The implementation of this Directive establishes a similar legislative model in all the European Union member states. The Directive states that users must opt in to receive unsolicited electronic communications for marketing purposes (Sipior, Ward & Bonner 2004, 62). Countries where "Opt-in" legislation has been enacted include Austria, Denmark, Finland, Germany, Greece, Hungary, Italy, Norway, Poland, Slovenia, and Spain. Countries where "Opt-in" legislation is under consideration include Belgium, France, and Sweden. Finland, France and the UK do not require opt-in when the recipient is a registered legal person (Sipior Ward & Bonner 2004, 62).

This Directive should be interpreted together with the 'general' Directive 95/46/EC, where concepts like consent, etc. are defined. In addition, other European Community law provisions may be applicable to unsolicited communications in relation to e.g. misleading advertising, harvesting, hacking.¹

In the Asia-Pacific region, Australia has been the first to introduce opt-in explicitly in their law. The NOIE Report recommending opt-in legislation was followed by the adoption of the Spam Bill 2003 by the Australian Parliament. Australia exempts government bodies, political parties, religious organisations, charities and educational institutions from respecting the opt-in requirement. There is no specific regulation on Spam in Canada to date, though an opt-in approach has been adopted by applying existing law. In Canada, under the Personal Information Protection and Electronic Documents Act electronic mail addresses are considered personal information. Thus, the collection and use without consent of personal information, such as E-mail address, could run counter to the requirements of the Act (Industry Canada 1999). Recent changes to the Federal Law of Consumer Protection in Mexico reflect the adoption of an opt-out approach. Mexican consumers are entitled to prevent specific businesses from disturbing them at home or at the workplace, or via E-mail, and from unauthorised transmission of personal data to third parties. To date, Korea and Japan have adopted an opt-out approach. However, the Ministry of Information and Communication (MIC) in Korea announced the introduction of opt-in for mobile phone services.

The 2004 US CAN-SPAM Act² took effect, which superceded more than 30 state law covering Spam. The legislation adopts an opt-out approach. Section 5 of the Act requires the following that all commercial E-mail must contain a valid opt-out mechanism, opt-out requests must be honored within 10 business days, sender must include a valid physical postal address, E-mail must provide a clear notice that it is an advertisement, E-mail must provide an operative return address, senders must avoid false, deceptive, or misleading E-mail transmission information or subject lines, and that senders must label sexually-oriented messages.

1.2 Economic analysis of different models

Opt-out approach is based on the idea of limited right of Spammers to send Spam. The central economic argument for this approach is

¹ For example, Directive 2000/31/EC, which includes provisions for transparency in relation to E-mail marketing, notably requiring that commercial communications must be identifiable as such.

² "Controlling the Assault of Non-solicited Pornography and Marketing Act", CAN-SPAM Act of 2003 (Pub. L. 108-187, S. 877).

cost reduction of the opt-out process. It does not take into account the possibility of a social loss when Spamming is done inefficiently. Neither does it induce Spammers to send Spam in an efficient manner (Coalition Against Unsolicited Commercial E-mail 2001; Scruggs & Anderson 1999). From an economic point of view, opt-out is only efficient under very strict conditions. The opt-out approach is usually inefficient (Khong 2004).

Under the opt-in approach, Spammers do not have a right to send unsolicited Spam, and this right is protected by a property rule. Taken that statutory or punitive damages are high enough to compensate for rational apathy, Spammers are induced not to send unsolicited Spam (Khong 2004). If E-mail users as a group could negotiate in a Coasean way with the Spammer, an efficient outcome can be achieved. But because E-mail users are a large and dispersed group, organizing them is costly (Khong 2004). For the same reason, opt-in laws are not common because of the inability of E-mail users to organize as a pressure group. The result is the same if advertising yields increasingly returns to scale. Spam is still not social welfare maximizing, although welfare is increased compared to the previous case. This is so because the gains by subscribers are not internalized by the Spammer (Khong 2004). As Gahran (2000) summarized that, the main advantages of opt-in e-mail services are timeliness, convenience, and control.

2 Labelling

Labelling consists of displaying standard identifying labels in the subject line or header such as "ADV" (advertisement), "ADLT" (adult-only; if it concerns material intended for those 18 years of age and older). With regard to labelling, Finland, Japan, Korea, Norway, Poland, the UK, and the US require senders to label certain kinds of messages, but others like Australia, Denmark, France, Germany, and Italy do not require it.

Many states in the US require a label in the subject line of an E-mail that will alert recipients that the message is an advertisement. This includes three modes: unsolicited sexually explicit messages must contain a label of "ADV: ADULT", "ADV: ADLT", "ADULT ADVERTISEMENT", "ADV: ADULT ADVERTISEMENT" at the beginning of the subject line;¹ unsolicited commercial E-mail messages must contain a label of "ADV:" or "ADVERTISEMENT".² The laws prohibit false, deceptive, or misleading subject lines.³

3 Identity

Regulation may include the prohibition of false sender identities or addresses; false headers or misleading information in the subject line, or disregarding an opt-out request through technical manipulation; unauthorised access or falsification of routing information or misrepresentation of information related to the identification of the point of origin or the transmission path; and the use of a third party's Internet domain name without permission.

Concerning the real identity of senders, the provision of opt-out in messages, and false information in headers and messages, quite a few countries have similar approaches. Australia, Belgium, Italy, Mexico, Netherlands, and Poland, indicated requiring the real identity and real address of a sender in their messages. The situation is similar regarding the opt-out requirement in messages. Denmark, Finland, Germany, Italy, Korea, and the UK have a regulation in which opt-out is required in messages so that recipients are able to oppose receiving further messages from the sender. France, Mexico, Norway and Poland do not require this. A number of countries prohibit false information in headers and messages, including Australia, Denmark, France, Italy, Poland and the US.

In the US, some states have taken steps to criminalize the act of sending unsolicited bulk E-mail containing false, falsified or missing routing information, or misrepresent or obscure the point of origin or routing information.⁴ Some states prohibit the sale, distribution, and possession with intent to sell software that is designed to falsify routing information.⁵ Some states outlaws unsolicited commercial E-mail using a third party's Internet address or domain name without permission.⁶ Some states require that the unsolicited commercial E-mail must include the sender's name, street address, and E-mail address, along with opt-out instructions.⁷

4 Address harvesting and do-not-Spam list

Harvesting E-mail addresses from websites can be prohibited and software products used for collecting E-mail addresses, transmitting bulk E-mail and falsifying return addresses (Spamware) can be banned or controlled. Regarding the use of Spamware, Australia, France, Italy, Japan,

1 As in Alaska, Arkansas, Illinois, Indiana, Kansas, Louisiana, Maine, Minnesota, Missouri, New Mexico, North Dakota, Oklahoma, Pennsylvania, South Dakota, Tennessee, Texas, Utah, and Wisconsin.

2 As in Arizona, Colorado, Michigan, and Nevada.

3 As in Arizona, Illinois, Indiana, Kansas, Maryland, Minnesota, Missouri, North Dakota, Oklahoma, Pennsylvania, South Dakota, Texas, Washington, West Virginia, and Wyoming.

4 As in Arizona, Arkansas, Colorado, Connecticut, Delaware, Illinois, Indiana, Iowa, Kansas, Louisiana, Maine, Maryland, Michigan, Minnesota, Nevada, North Carolina, North Dakota, Ohio, Oklahoma, Pennsylvania, Rhode Island, South Dakota, Tennessee, Texas, Utah, Virginia, Washington, West Virginia, and Wyoming.

5 As in Arkansas, Connecticut, Delaware, Illinois, Kansas, Louisiana, Michigan, Nevada, Oklahoma, Pennsylvania, Rhode Island, Tennessee, Virginia, and West Virginia.

6 As in Arizona, Arkansas, Colorado, Idaho, Illinois, Indiana, Iowa, Kansas, Maine, Maryland, Minnesota, North Dakota, Oklahoma, Pennsylvania, Rhode Island, Texas, Washington, West Virginia, and Wyoming.

7 Arkansas, Colorado, Indiana, Iowa, Kansas, Maine, Minnesota, Missouri, Nevada, New Mexico, Ohio, Oklahoma, Rhode Island, Tennessee, and Utah.

Korea, and Spain have a regulation which prohibits the use of Spamware for the purpose of Spamming, while others such as Denmark, Finland, Germany, and the UK do not. The US prohibits the harvesting of E-mail addresses, dictionary attacks and spoofing.

With regard to do-not-Spam lists, most countries do not require the operation of do-not-Spam lists, with the exception of Austria and Korea. However, the UK, even though it is not a statutory requirement, opt-out registers have been operated under industry codes of practice.

5 Criminal sanctions and civil remedies

5.1 Criminal sanctions

Sanctions for violation of Spam laws and regulations are getting tougher. Some countries such as Korea have considerably increased existing fines imposed on Spammers by amending existing regulations. Others like Italy impose not only fines on Spammers but also prison terms (OECD 2004).

In some of the US states, Spam has been criminalized by state laws, such as Colorado, Nevada, Pennsylvania, Connecticut, Delaware, Louisiana, North Carolina, and Virginia. In some other jurisdictions without statutes regulating commercial Spam, unsolicited E-mail is usually regulated with reference to harassment, stalking, and sexually explicit communication to minors, such as in Hawaii, Wisconsin, and Maryland. The Section 4 of 2004 CAN-SPAM Act prohibits hiding E-mail origin using other computers (hacking and relaying), false or misleading E-mail header information, deception in registration of E-mail and domain names, and ownership of IP addresses. Under the Act, violations of the provisions above can result in fines and imprisonment of between 1 and 5 years depending on the seriousness of the violation and other factors. Section 4 of the Act provides for forfeiture of property used in connection with the commission of the offense, or gained in or traceable to the commission of the offense.

In exploring the sanctions for Spam, there are two problems deserving reconsidered.

First, it is generally argued that the fine is better than imprisonment for several reasons, assuming the deterrence costs are the same (See generally Garoupa 2003). If the hacker works, he will learn some new skills and perhaps be able to become more attached to the legitimate labor market (See generally Garoupa 2003). However, given that they are long specified in computer science, and deprived the chances of further study, their knowledge and skills will become outdated after several months or years. If the fine is used to compensate the Spam victims, then their loss will be reduced, and the cost to society of his or her crime will be reduced. This is more efficient than having him or her in jail, which doesn't help the victims (See generally Garoupa 2003). However, in the case of Spam, there are always too many victims (thousands or millions), it is impossible to pay each victim. Thus, the loss of the victim become a pure social loss, and cannot be recovered from the criminal.

Second, prosecutors face a number of costs when bringing legal action against Spammers. The cost of tracking down Spammers, the costs of actually litigating a trial once a target has been identified, and any negative externalities borne by society as a result of prosecution, the cost to those legitimate businesses must be taken into account (Prince 2004). The expected effectiveness of an anti-Spam law is determined by a number of quantifiable factors, such as the potential benefit to society from a single successful prosecution, the costs of identifying a Spammer to be prosecuted and the costs of actually bringing the prosecution against him or her, the likelihood of success at trial, and any external costs to society that arise as a byproduct of prosecution (Prince 2004). In order to justify prosecuting a Spammer, the expected effectiveness quotient must be as high as possible (Prince 2004). For an anti-Spam law to be a successful deterrent to Spammers, it must be drafted to increase the benefit from a successful prosecution, decrease the cost of identifying a Spammer, decrease the cost of prosecution, increase the probability of success at trial, or decrease any external costs to society from investigating and bringing a trial (Prince 2004).

Although there are cases of harsh criminal sanctions such as that a Virginian spammer was sentenced to 9 years in prison for sending 10 million E-mails each day, and cases of large damages, such as that another spammer was sued by AOL for 7 million dollar, Spamhaus estimates that by the summer of 2006 spam will account for 95% of all e-mails sent and the problem will not be alleviated (Wakefiled 2005).

5.2 Civil remedies

It is also possible to take civil actions against spam senders. First of all, because the ISPs' systems are repeatedly burdened by huge volume mailings, they can incur noteworthy cost. Thus, they have the choice of seeking financial compensation through civil action. Generally, civil laws that apply to damages resulting from wrongful actions or breaches of contract would apply to conventional and online activities equally. The scope of contract liability is largely a matter for ISPs and other intermediaries, who are free to set the terms of contracts with their subscribers. Many existing contracts incorporate anti-spamming conditions (Ferguson & Piragoff, 1997).

Another form of civil actions can also protect recipients from Spamming. Damages are a good deterrent against spam. Laws of some the US states provide statutory damages to individuals and ESPs. These damages vary from US\$10 per message in Colorado and Iowa to US\$500 in Rhode Island. Some states also allow recovery of actual damages to spam recipients and network administrators. Section 5 of the US CAN-SPAM Act. Although the Act does not provide a civil cause of action for individuals against Spammers, it empowers attorneys general of each state to pursue violators of certain parts of Section 5 on behalf of the residents of its state. A state attorney general can pursue money damages, injunctive relief to stop further violations of the Act, or statutory damages which can total to \$2,000,000 or more for inclusion of false or misleading transmission information, or if circumstances support a finding of aggravated damages. Statutory damages can reach up to \$250 per address to which an E-mail is sent. A court may treble damages if it finds aggravating circumstances, and may in its discretion award attorney

fees for successful actions. Others who have a civil cause of action under the Act include ISP's and certain federal agencies. ISP's are provided a civil cause of action against violators of certain sections of the Act. Finally, the Act generally can be enforced by a variety of federal agencies noted in the Act when the actions or actors fall within the agency's purview.

6 International co-operation

As a global problem, the practical problems in finding wrongdoers, establishing jurisdiction, and enforcing remedies, investigation and prosecution of cases involving Spam are extremely difficult. The different approaches among countries may cause further difficulties to implement effective solutions worldwide. The Spam outside their territories will be outside their reach.

There have been a number of international initiatives to address the problem of cross-border scams. In particular, in June 2003, the OECD adopted new guidelines to foster international co-operation against cross-border fraud and deception (OECD 2003). Spam messages that contain deceptive or fraudulent representations may fall within the scope of the guidelines, offering the prospect of putting into play the framework for enforcement co-operation outlined by the guidelines.

Recent trends in international co-operation have been between industries, organisations and the consumer or citizen, and between industries and government. Important multi-lateral organisations include the OECD, ITU, APEC, ICANN and ICPEN. International co-operation which is multi-pronged needs to include various different communities in order to be effective (OECD 2004). In dealing with the problem of Spam, the new-styled international co-operation is an urgent call. As of 2005, International Council on Internet Communications was formed to coordinate international efforts to stop spammers (NewsTarget 2005). Given Spam is still in its rapid developing stage, we cannot expect any of such institutions are able to solve the problem in a predictable period.

7 Regulatory solution revisited

The fact that the amount of Spam is rising despite the number of world legislations restraining it suggests that legislation is not a sure solution to the Spam problem. Certain regulations, such as a labeling "ADV" in message headers, have not proven effective (FTC 2003b). Some organizations such as the Direct Marketing Association (DMA) argue that only legitimate law-abiding marketers would actually use ADV labeling, which voluntarily subjects them to mass filtering. Others also question the effectiveness of government-operated nationwide "do-not-E-mail registries", because such lists would only punish those reputable marketers who comply with them. On the other hand, opt-out is not used by most consumers, who fear that opt-out will confirm their address to Spammers; uncertainty as to whether opt-out will work; doubt that opt-out will be honored (ePrivacy Group 2003).

There are a number of limitations to the effectiveness of law enforcement against Spamming. These include low cost-effectiveness, difficulty in tracking Spammers, difficulty in collecting evidence across borders, varying regulations between states or countries, etc. Some interpretations of existing privacy legislation can also raise obstacles to effective law enforcement, if they do not allow law enforcement to have access to information about alleged Spammers.

Since the first anti-Spam law worldwide was passed in 1997, at least 75 governments around the world have passed anti-Spam laws (Sorkin 2004; Direct Marketing Association 2004). The empirical evidence for the failure is quite clear. In 1997, the average e-mail user received approximately one unsolicited commercial e-mail message per week (Cranor & LaMacchia 1998). By 2003, the average e-mail user received 25 such messages daily (InsightExpress/UnSpam 2003) While that is an astounding 175-fold increase in merely six years, the averages vastly underestimate the problem for many active e-mail users, some of whom receive literally thousands of Spam messages each day (InsightExpress/UnSpam 2003) Spammers routinely flout the law because the risk of prosecution is so low. Three months after the passage of the US CAN-SPAM Act,¹ only three per cent of Spam messages complied with its requirements (McGuire 2004). What is worse is that today the compliance rate is down to a scant one per cent (McGuire 2004). More pessimistic perspective shows that "*Law Barring Junk E-Mail Allows a Flood Instead*" (Zeller 2005). According to Jared Blank, "The laws are nice in theory, but actually going after and tracking down spammers is extraordinarily difficult." (Levine 2003).

VIII Conclusions

Spammers are motivated by benefits from spamming that are greater than other kind of direct mailing. Any previous single solution cannot work alone to solve the problem. Comprehensive mechanisms must be established to protect the recipients with more effective anti-Spam systems, and to impose criminal and civil liability on the sender.

References

1. Ayres, I., & Nalebuff, B. (2003). Want to Call Me? Pay Me! In *Wall Street Journal*, 8 Oct. 2003.
2. Batista, Elisa. (2000). A Fight to Ban Cellphone Spam, *Wired News*, 6 July 2000.
3. Becker, G. (1968). "Crime and Punishment: An Economic Approach," *Journal of Political Economy* 76, 169-217.
4. Blum, M., von Ahn, L. A., Langford, J., & Hopper, N. (2000). The CAPTCHA Project: Completely Automatic Public Turing Test to Tell Computers and Humans Apart, Nov. 2000, at <http://www.captcha.net> (accessed 28 April 2005).
5. Boldt, Martin, Carlsson, Bengt, & Jacobsson, Andreas. (2004). Exploring Spyware Effects, at http://psi.bth.se/mbo/exploring_spyware_effects

¹ See 15 USC. § 7705. CAN-SPAM stands for the "Controlling the Assault of Non-Solicited Pornography and Aggressive Marketing." It was signed into law 16 Dec. 2003 and became effective 1 Jan. 2004.

nordsec2004.pdf (accessed 28 April 2005).

6. Coalition against Unsolicited Commercial E-mail. (2001). CAUCE Does the Math—Why Can't the Marketing Industry? 15 May 2001, at <http://www.cauce.org/pressreleases/math.shtml> (accessed 28 April 2005).
7. Cobb, Steven. (2003). The Economics of Spam, at http://www.spamhelp.org/articles/economics_of_spam.pdf (accessed 28 April 2005).
8. Cooley, A. L. (2004). The Cocktail Approach to Spam Protection, Network Security White paper.
9. Cranor, L. F. & LaMacchia, B. A. (1998). Spam! Communications of the ACM. 41(8), pp. 74-83.
10. Dem, Daniel P. (1998). Postage Due on Junk E-mail: Spam Costs Internet Millions Every Month, Internet Week, 4 May 1998.
11. Direct Marketing Association, Executive Summary of International Spam Laws, at <http://www.the-dma.org/antispam/spamlaws.html> (accessed 28 April 2005).
12. Dwork, C., & Naor, M. (1993). Pricing via Processing or Combating Junk Mail. In Lecture Notes in Computer Science 740 (Proceedings of CRYPTO'92), pp. 137-147, 1993.
13. Dwork, C., Goldberg, A., & Naor, M. (2003). On Memory-bound Functions for Fighting Spam, Proceedings of the 23rd Annual International Cryptology Conference (CRYPTO 2003), pp. 426-444, Santa Barbara, CA, Aug. 2003.
14. Equip Technology and CipherTrust. (2004). Spam and Productivity Theft- a Growing Concern for UK PLC. A Report by Equip Technology and CipherTrust, at <http://www.apig.org.uk/equipandciphertrustevidence.doc> (accessed 28 April 2005).
15. Fahlman, S. E. (2002). Selling Interrupt Rights: A Way to Control Unwanted E-mail and Telephone Calls. IBM Systems Journal, 41(4):759-766, 2002.
16. Federal Trade Commission, National Do-Not-E-mail Report to Congress, 15 June 2004.
17. Federal Trade Commission. (1998). FTC Names Its Dirty Dozens: 12 Scams Most Likely to Arrive via Bulk E-mail, FTC Consumer Alert, July 1998.
18. Ferguson, Peter, & Piragoff, Donald K. (1997). Internet and Bulk Unsolicited Electronic Mail, at [http://e-com.ic.gc.ca/epic/internet/inecic-ceac.nsf/vwaj/SPAM_1997En.pdf/\\$FILE/SPAM_1997En.pdf](http://e-com.ic.gc.ca/epic/internet/inecic-ceac.nsf/vwaj/SPAM_1997En.pdf/$FILE/SPAM_1997En.pdf) (accessed 28 April 2005).
19. Foster, Ed. (2000). Viral Marketing Goes One Step too Far—To a Place Where Friends Spam Friends, InfoWorld, 7 Feb. 2000.
20. Gahran, Amy. (2000). Investor relations Content that Works, 10 March 2000, at <http://www.contentious.com/articles/V2/2-7/feature2-7.html> (accessed 28 April 2005).
21. Garoupa, Nuno. (2004). An Economic Analysis of Criminal Law, at http://esnie.u-paris10.fr/pdf/textes_2004/Garoupa_criminalaw01.pdf (accessed 28 April 2005).
22. Gartner Consulting. (1999). ISPs and Spam: The Impact of Spam on Customer Retention and Acquisition, Gartner Consulting, 14 June 1999.
23. Gauthronet, Serge, & Drouard, Etienne. (2001). Unsolicited Commercial Communications and Data Protection (Brussels: Commission of the European Communities, Internal Market Directorate General, 2001), Contract no. ETD/99/B5-3000/E/96.
24. Goodman, Peter S. (2000). Verizon Online User's E-mail Problems Persist, Washington Post, 13 Dec. 2000, p. E01.
25. Griffin, P. (2003). Spammers Remain Unrepentant as They Make Money, in the New Zealand Herald, 21 March 2003.
26. Grimes, Anne. (2003). Digits: Spam pays, The Wall Street Journal, 22 May 2003, p. B3.
27. Hansell, Saul. (2003a). Internet is Losing Ground in Battle against Spam. The New York Times. 22 April 2003, p. 1.
28. Hansell, Saul. (2003b). The High, Really High or Incredibly High Cost of Spam, The New York Times, 29 July, 2003.
29. Hise, Phaedra. (1999). Mom Spam: The Cyber-Scourge of Families Everywhere, Salon, 20 Dec. 1999, at <http://www.salon.com/mwt/feature/1999/12/20/Spam/> (accessed 28 April 2005).
30. IMT Strategies (2001). Raising the Stakes in Permission Marketing, Stamford, CT USA, at <http://www.imtstrategies.com/download/TI13.01.pdf/> (accessed 28 April 2005).
31. Industry Canada. (1999). Internet and Bulk Unsolicited Electronic Mail (SPAM) Policy, July 1999, at <http://e-com.ic.gc.ca/epic/internet/inecic-ceac.nsf/vwGeneratedInterE/gv00188e.html> (accessed 28 April 2005).
32. Infoworld. (2003). What is the Worst IT Disaster of the Last Year, July 2003.
33. InsightExpress/UnSpam. (2003). Comprehensive Spam Survey, 12 Oct. 2003, at http://www.unSpam.com/fight_Spam/information/survey_personal.html (accessed 28 April 2005).
34. ITU (International Telecommunication Union). (2004a). Meeting Announcement: ITU WSIS Thematic Meeting on Countering Spam, CICG, Geneva, 7-9 July 2004.
35. ITU (International Telecommunication Union). (2004b). Council Working Group on the World Summit on the Information Society, Document WG-WSIS 7/13-E, 2004.
36. Johansson, E. S. (2002). Camram, 2002, at <http://www.camram.org> (accessed 28 April 2005).
37. Kelly, J.S. (2002). A Brief History of Spam, at <http://www-106.ibm.com/developerworks/linux/library/l-spam/l-spam.html> (accessed 28 April 2005).
38. Khong, D.W.K. (2004). An Economic Analysis of Spam Law, Erasmus Law and Economics Review, 1 (Feb. 2004): pp. 23-45.
39. Kraut, R., Sunder, S., Morris, J., Cronin, M., & Filer, D. (2003). Markets for attention: Will postage for E-mail help? In ACM Conference on CSCW, pp. 206-215, 2003.
40. Kraut, R.E., Sunder, S., Telang, R., & Morris, J. (2004). Pricing Electronic Mail to Solve the Problem of Spam, at <http://www.econ.upf.es/docs/seminars/sunder.pdf> (accessed 28 April 2005).
41. Levine, Jessica. (2003). Spam and the Law, PC Magazine, 25 Feb. 2003.
42. MAPS (Mail Abuse Prevention System). (2004). Definition of Spam, at <http://www.mail-abuse.com/Spam-def.html> (accessed 28 April 2005).
43. Marlin, A.S. (2000). First Amendment Is Obstacle to Spam Legislation, CNN.com, at <http://archives.cnn.com/2000/TECH/computing/06/09/amend.spam.idg/index.html> (accessed 28 April 2005).
44. McGuire, David. (2004). Report: More Spam Violates Law, Washington Post, 9 June 2004.
45. Moran, J. M. (2002). Spam King Living High in the Bayou, in The Hartford Courant, 30 June 2002.
46. Naor, M. (1996). Verification of a Human in the Loop or Identification via the Turing Test, at <http://www.wisdom.weizmann.ac.il/~naor/PAPERS/>

(accessed 28 April 2005).

47. NewsTarget. (2005). New international anti-spam council pledges to fight spam around the world, 28 April 2005, at http://www.wired.com/news/technology/0,1282,64383,00.html?tw=wn_tophead_5 (accessed 28 April 2005).
48. Niall, Jim (2000). The E-mail Marketing Dialogue, Forrester Report, Cambridge.
49. OECD. (2003). OECD Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices Across Borders, June 2003.
50. OECD. (2004). 2nd OECD Workshop on Spam: Report of the Workshop. JT00174847.
51. Peppers, D. & Rogers, M. (2000), E-mail Marketing Maximized, Peppers, Stamford, C.A.
52. Pool, I., Inose, H., Takasaki, N. & Hurwitz, R. (1984). Communication flows: A Census in the United States and Japan. New York: North-Holland.
53. Prince, M. (2004). How to Craft an Effective Anti-Spam Law, June 2004, at <http://www.itu.int/spamH> (accessed 28 April 2005).
54. Radical group, The Radical Group, Inc. Release Q1 2005 Market Numbers Update, 25 April 2005.
55. Sahami, M., Dumais, S., Heckerman, D., & Horvitz, E. (1998). A Bayesian Approach to Filtering Junk E-mail. In AAAI '98 Workshop on Learning for Text Categorization, July 1998.
56. Scruggs, D., & Anderson, H. (1999) Sometimes the Messenger Should Be Shot: Building a Spam-free E-mail Marketing Program, 1999, at <http://www.messagemedia.com/> (accessed 28 April 2005).
57. Simon, H. A. (1982). Designing Organizations for an Information-rich World: Models of Bounded Rationality, MIT Press. pp. 171-185.
58. Sipior, J. C., Ward, B. T., and Bonner, P. G.. (2004). Should Spam Be on the Menu? Communications of the ACM, vol. 47, no. 6, 59-63 (June 2004).
59. Sorkin, David E. (2004). Spam Laws, at <http://www.spamlaws.com/> (accessed 28 April 2005).
60. Templeton. (2003). Origin of the Term "Spam" to Mean Net Abuse, at <http://www.templetons.com/brad/spamterm.html> (accessed 28 April 2005).
61. Wakefiled, Jane, UK laws are failing to deter spam, BBC News, 21 April 2005, at <http://news.bbc.co.uk/1/hi/technology/4466053.stm> (accessed 28 April 2005).
62. Wendland, M. (2002). Spam King Lives Large off Others' E-mail Troubles, in The Detroit Free Press, 22 Nov. 2002.
63. Wreden, N. (1999), Mapping the Frontiers on E-mail Marketing, Harvard Management Communication Letter, 9 Jan. 1999.
64. Wright, N. D., & Bolting, C. P. (2001), Marketing via E-mail: Maximizing its Effectiveness Without Resorting to Spam, working paper, James Madison University.
65. WSIS (World Summit of Information Society). (2003). Declaration of Principles-Building the Information Society: a Global Challenge in the New Millennium, World Summit of Information Society, 2003.
66. Zandt, T. V. (2003). Information Overload in a Network of Targeted Communication, RAND.
67. Zeller, T., Jr. (2005). Law Barring Junk E-Mail Allows a Flood Instead, New York Times, [nytimes.com](http://www.nytimes.com), Feb. 2005.
68. Wikipedia, Externalities, at <http://en.wikipedia.org/wiki/Externality> (accessed 28 April 2005).
69. Amaditz, K. C. (1999). Canning "Spam" in Virginia: Model Legislation to Control Junk E-mail, Virginia Journal of Law and Technology, Vol. 4, Issue 4, 1999.

Cyber Warfare: Jokes, Hoaxes, or Hypes?

Abstract: Cyber warfare is increasingly listed alongside nuclear, chemical, and biological weapons as a potential weapon of mass destruction. Interest in and concerns for cyber warfare have also been prevalent for decades. War-oriented writer usually exploited such serious and expensive terms as cyber war, information war, and electronic war to spread their impetuous and cheap ideas. This essay by no means devalues serious designs and plans, studies and research, ideas and claims revolving around cyber warfare. Rather, the purpose of this paper is to analyze existing jokes, hoaxes and hypes on the so-called cyber warfare, so as to distance serious research from misleading information.

Keywords: Cyber warfare, cyberspace, cybercrime, cyber law, cyber security

Introduction

While we are enjoying the fruits of the possibility of disseminating information in large quantities and at high speed in this networked society, we have also to take the risk of forcing ourselves to trade unexpected by-products of cyberspace. Information and communications technology (ICT) can produce a surprisingly large amount of products and by-products for these technology-dependent people, such as security and insecurity, welfare and crime, peace and war, to name some. In fact, insecurity, crime and war are information society's silhouettes, merging easily but being difficult to eliminate.

Overall, the Internet services lack of controllability and become the breeding ground of insecurity, as a response to which many governments have enacted specific legislation criminalizing invasive and destructive activities targeted at information systems. Because security-breaking activities, committed with the assistance of the

globally-connected computer networks, can easily cross the territorial borders, it is unknown but broadly accepted that different countermeasures may generate a paradise for perpetrators.

Information Warfare (IW) is increasingly listed alongside nuclear, chemical, and biological weapons as a potential weapon of mass destruction (WMD)—or at least as a weapon of mass disruption (Eriksson 1999, pp. 57-64). Under such circumstances, interest in and concern for cyber warfare have also been prevalent for decades. War-oriented writer usually exploited such serious and expensive terms as cyber war, information war, and electronic war to spread their impetuous and cheap ideas. Using search engines, we can produce the following numbers of results (as of July 17, 2009):

Table 1 Online Use of Cyber War Terms

	Google	Yahoo	Amazon (copies of books only)
Cyber war	121,000,000	55,600,000	697
Cyberwar	1,770,000	4,740,000	718
Cyber warfare	840,000	11,100,000	549
Cyberwarfare	315,000	2,890,000	278
Information war	1,140,000,000	875,000,000	26,445
Information warfare	94,800,000	59,100,000	4,594

It may be said that the terms are used in a way blotting out the sky and the earth in cyberspace. Yet worse, authors created scores of books in the title of which filled with such terms as well, mostly without critical views against the abuse of them. Information society, to some extent, means there is too much information for users to consume, so that they are frightened by cyber war and cyber terror, victimized by cyber bullying and cyber crime, and at last jammed by cyber jokes, cyber hoaxes and cyber hypes.

As a computer and network security researcher and industry leader, Marcus J. Ranum said in March 2009,

“There has been a great deal of irresponsible and inaccurate talk about ‘Cyber War’ in the last decade in spite of the fact that it’s technologically and militarily impractical. Its counterpart, ‘Cyber Espionage’ makes a bit more sense, and is less mythical but falls under the category of ‘nothing new.’”

Nevertheless, there are still few people realizing the real issue behind media’s full coverage of cyber attack during big or small international conflicts. No more than a month ago, it was reported that Britain’s Security Minister, Lord West, as he published the Government’s Cyber Security Strategy, had issued a warning about terrorists’ intentions of launching a cyber warfare battle against the UK (Gardham 2009).

The strategy clarified in detail the threats from various actors. Besides criminals,

“The most sophisticated threat in the cyber domain is from established, capable states seeking to exploit computers and communications networks to gather intelligence on government, military, industrial and economic targets, and opponents of their regimes. The techniques used by these state actors go beyond ‘traditional’ intelligence gathering and can also be used for spreading disinformation and disrupting critical services...Some states also encourage, and benefit from, the expertise of ‘patriotic hackers’...carrying out attacks safe from prosecution in their own countries. The use of proxies provides state actors with an extra level of deniability”. (UK Office of Cyber Security and UK Cyber Security Operation Centre 2009, p. 13)

“Terrorists and violent extremists use cyber space for communication, co-ordination, propaganda, fundraising, radicalisation, and recruitment...Whilst we expect terrorist groups to continue to favour high-profile conventional operations over cyber attacks, we must be vigilant against any future increase in capability...” (UK Office of Cyber Security and UK Cyber Security Operation Centre 2009, p. 13).

A growing tendency is that many writers have recognized the pseudomorphism of the cyber warfare hallucination, revealing the truth and interest behind cyber warfare claims. This essay by no means devalues serious designs and plans, studies and research, ideas and claims revolving around cyber warfare. Rather, the purpose of this paper is to analyze existing jokes, hoaxes and hypes on the so-called cyber warfare, so as to distance serious research from misleading information. Serious researchers should

always bear in mind that the use of information on cyber warfare in today's world is a thing that needs reliable evidence, proof and witnesses.

How to write “the scariest cyber warfare article”

Cyber warfare has become a big topic, an attractive topic, a revenue-generating topic, and a hot topic. Readers and audience are willing to read, listen and watch however it is written, narrated and performed. Authors are willing to write whatever the readers are willing to read. Media are willing to publish whatever the authors are willing to write and whatever the readers are willing to read. Every player meets his/her own needs in one way or the other: readers satisfy their endless curiosity by reading, writers make their money by writing, and media win both popularity and money from publishing, and government shows up its political achievements. Even the army will demonstrate their ability and capacity by presenting their understanding of and deal with the “big” issue, which is something a mystery for layman. However, any discourse has to have some structural expression, beginning with attraction, processing with ambiguity, and ending with suspense. Yet everything should not be so accurate, so sound, so clear, and so sure.

Therefore, when we read almost all of the news reports and articles by non-academic authors, we have the strong feeling that these articles can be composed by everyone who is willing to do so. Reality, fact, truth, accuracy and conscience are not so relevant here. The only things are some tips that should be followed. Evgeny Morozov published his guidance on “10 easy steps to writing the scariest cyber warfare article ever” (Morozov, 2009a). There, he sarcastically proposed some tips on how a cyber warfare article can be manufactured. Key things to be presented are: digital Pearl Harbor, 2007 attacks on Estonia, Chinese hackers, cyber-pranks, expert quotations, old stories, etc. By doing so, a cyber warfare article can be concocted in a low-cost high-benefit efficient way.

His steps are (seemingly only 9 steps, with original step 7 missing. Here they are re-numbered):

1. Give a catchy title with coined terms such as “digital Pearl Harbor”, “cyber-Katrina”, and “electronic 9/11”, but never explain what it means;
2. Begin the story with 2007 attacks on Estonia, but never mention that it only lasted for twenty minutes;
3. Drop references to Chinese hackers in every paragraph;
4. Mention the cyber-pranks of Kremlin-affiliated youth movements;
5. Find and quote industry experts with the biggest possible conflicts of interest;
6. Go and recycle old facts, quotes, and official statements;
7. Throw in some geopolitical kerfuffle that involves a country located between China and Russia;
8. Refer to anything involving cyber war between Israel and Palestine;
9. Make sure to mention that NSA, CIA, and DIA are all involved in the case, but they cannot comment.

In a word, writing about cyber warfare could not be done by delicate scientific calculation, detailed statistics, real-life interview, deep investigation, and field work in person. It should be developed through imagination under some kinds of inspiration. It is like a sci-fi rather than a fact report.

Practically, among others, every article published in recent three years began with 2007 cyber attacks on Estonia, which has already been proved to be the act of a native ethnic Russian young man. No nation state was ever involved. No government was behind him. No official coordination ever took place. Yet they suspected a country from beginning to the end. Furthermore, authors tend to connect every catastrophic result in critical infrastructure in the real world with possibility of interruption of the Internet. As typical articles started the narration in this way:

“Imagine that agents of a hostile power, working in conjunction with organized crime, could cause huge traffic jams in your country's biggest cities-big enough to paralyze business, the media, government and public services, and to cut you off from the world. That would be seen as a grave risk to national security, surely? Yes, unless the attacks came over the internet.” (Economist, 2007).

“The next world war might not start with a bang, but with a blackout. An enemy could send a few lines of code to control computers at key power plants, causing

equipment to overheat and melt down, plunging sectors of the U.S. and Canadian grid into darkness. Trains could roll to a stop on their tracks, while airport landing lights wink out and the few traffic lights that remain active blink at random.

“In the silence and darkness, citizens may panic, or they may just sit tight and wait for it all to reboot. Either way, much of the country would be blind and unresponsive to outside events. And that might be the enemy’s objective: Divert America’s attention while mounting an offensive against another country.” (Derene, 2009)

In fact, events in cyberspace could never be compared with their social counterparts. No one has reportedly died of hacking, spamming or stalking. No company has reportedly bankrupted due to denial-of-service attacks. Even the broadly concerned Nigerian 419 scam has never had as big a business as done by the former chairman of the Nasdaq stock market. It seems that when people are unable to deal with issues in front of them, then they will look for some scapegoat, regardless of offline or online, so that the issue can be enlarged at such a scale that it seems cannot be dealt with using normal efforts. As a result, they are to be excused. Then more sophisticated ideas will be written; what are written will be published; what are published will be read; what are read will surely benefit all. Government and the army will get more money from taxpayers and employ more personnel, construct bigger office buildings, be better respected by citizens. “Cyber warfare” discourse is helping to form a cost-effective new industry. As Morozov pointed out that,

“Cyber-security fears have had, it should be said, one unambiguous effect: they have fueled a growing cyber-security market, which, according to some projections, will grow twice as fast as the rest of the IT industry.” (Morozov, 2009b)

However, look at how media are trying to distance themselves from the author, even though they are pleased to harvest money from fake stories:

“Reader’s advisory: Wired News has been unable to confirm some sources for a number of stories written by this author. If you have any information about sources cited in this article, please send an e-mail to sourceinfo[AT]wired.com.” (Retrieved July 17, 2009 from <http://www.wired.com/politics/law/news/2001/04/43437>).

April Fool's joke

In early 1990s, during Gulf War I, Infoworld magazine published as April Fool's joke. The story claimed that the National Security Agency had developed a computer virus, called AF/91, to immobilize Iraqi air defense computers by chomping windows. What was mystified was that the virus was smuggled into Iraq through Jordan, concealed in a chip in a printer.

The joke was gossiped for days by those who thought it funny as well as those who missed the original citation and engaged in laborious discussion on the imagined technology of the virus (Smith, 2003). U.S. News and World Report acquired the story and published news of the Gulf War virus in its coverage of the war (Smith, 2003). The U.S. News and World Report wrote that the Gulf War virus attacked Saddam's defenses by "devouring windows" that Iraqi defenders used to check on aspects of their air defense system: "Each time a technician opened a window...the window would disappear and the information would vanish." From there, the fake story was reported by the Associated Press, CNN, ABC Nightline, and newspapers across the U.S. (Smith, 2003).

In probing the reason why the hoax could succeed, Smith (2003) pointed out that,

"The Gulf War virus plays to a uniquely American trait: a child-like belief in gadgets and technology and the people who make them as answers to everything. Secret National Security Agency computer scientists made viruses that hobbled Saddam's anti-air defense without firing a shot! Or maybe it didn't work but it sure was a good plan!"

Some years later, I heard another piece of news from radio, reporting that there emerged a kind of powerful influenza virus, which could reside in a telephone and spread via the telephone line to other telephones, regardless of however its length was. As soon as the call from the telephone where the viruses resided was accepted by the other side, the viruses could transport themselves along the line to the telephone where they did not yet reside by 300,000 kilometers per second, the velocity of light. It was a matter of picking the phone up. They came out now and then from the telephone they resided and infected people nearby. This humorous version of a horror, integrating both

natural phenomena and high-tech invention, can pose a more “realistic” threat against human beings than cyber warfare does. Just imagine it.

Rise and fall of Estonian cyber war hoax

“Estonia, a good place for an alleged cyberwar because no real journalists were actually interested in actually wasting their time in going there to investigate it, is a fine repeatable tale in the tradition of digital warstories.” (Smith 2007)

The term “Estonia under cyber attack” made many people to recall the breaking news broadcast on TV on September 11, 2001, when several planes flew into several U.S. buildings. The difference between them is that the Estonian version is a cyber attack. April of 2007 witnessed Estonian authorities’ relocation of the Bronze Soldier of Tallinn from the center of the capital city to the outskirts of town. Nationalists in that country considered the Soviet Red Army as occupiers and oppressors. Ethnic Russians, making up nearly a quarter of Estonia’s population, were incensed by the statue’s treatment and took to the streets in protest. Estonia later blamed Moscow for coordinating the turbulence; order was restored after American and European diplomatic interventions. Days after the riots, the information infrastructure of Estonia began to fray, victimized by “denial of service” attack. A flood of sham requests for information from computers around the world conspired to cripple the websites of Estonian banks, media outlets, and ministries for days. Estonia denounced the attacks as an unprovoked act of aggression from a regional enemy.

Some observers reckoned that the onslaught on Estonia was of a sophistication not seen before. The case is studied intensively by many countries and military planners as it may have been one of the largest instances of state-sponsored cyberwarfare.

Estonian Foreign Minister Urmas Paet accused the Kremlin of direct involvement in the cyber attacks. However, on September 6, 2007 Estonia’s defense minister admitted he had no evidence linking cyber attacks to Russian authorities. Russia called accusations of its involvement “unfounded,” and neither NATO nor European

Commission experts were able to find any proof of official Russian government participation.

In early 2008, one Estonian ethnic-Russian national has been charged and convicted. The so-called Estonia Cyber War turned out to be some Estonian citizens' activities. What an embarrassment for all those who had ever hyped such a case as a cyber war.

A “cyber warfare” years before

According to many journalists and analysts, “Cyberwar has always been said to be easy to do. Al Qaeda has always been said to be working on it. Before al Qaeda, it was Russia, China, India, North Korea. Even Saddam Hussein was imagined to be readying a US-smashing Internet strike force.” (Smith 2007)

In recent years, the so-called cyber warfare becomes a routine activity when ever international conflicts emerge. One of such occasion took place in 2001 when the world was in troubled times. Early that year, a scholar had launched a “cyber war” by himself and he was nearly criminally investigated. At the time, He was offered a scholarship to pursue studies and research on economic criminal law in a highly industrialized country, where the computer and networks had already been ubiquitously used. His office there was equipped with a computer and it got connected to the Internet.

Long before that, he had had some interest in doing further research on cybercrime, the counterpart of which, computer crime, had been the theme of his master's degree thesis.

Lawyers whose research was focused on legal issues in cyberspace generally did not probe the mechanism of these activities in detail. In this occasion, in order to better understand how the computer could be compromised, he decided to do a series of experiments. He made contact with some laboratories in West Europe and North America for potential opportunities to be hosted, but only in vain. Finally, he began to change his office into his own laboratory, using two notebook computers. The first step of his experiment was to test the security level of computers in several universities and

other institutions in several countries located in different continents, so that he could have first-hand knowledge about whether they were protected and to what extent they were secure. The experiment was done by using programs publicly available on the web. No one said whether such tools were legal or not. No one prohibited them from being created and disseminated. He just used such tools in his experiment to look for externally accessible computers online. Upon setup the parameters, the work was automatically done, with open ports listed. During a time span of around 10 days, he used his computers at work in day time, and left them doing the research in night time.

He took down each open vulnerable computer in a note book. After some days, hundreds of thousands of computers had been tested; hundreds of such computers had been found, including those in use at universities in that country and other countries. By this record, he could do quite a lot of analysis.

His work would have never been completed voluntarily as the result would surely have been of great value for his research.

However, all of a sudden, his computers were taken offline by the computer centre of the host university, and an investigation was set out firstly by a professor at the same faculty, who also did research on informatics.

According to the IP address assigned to me in advance, he visited his office and had a brief look at his laptops. He just confirmed that the suspected IP address was that had been used in the suspected attack.

As a response, he paid a visit to the professor's office soon after and explained his awkward work during the past days. The professor had opened an email message on his desktop screen, saying that the computer centre had noted abnormal activities from a computer with a certain IP address, which should have been assigned to a user at this faculty. The influence of this was that the abnormality exploited quite some the then scarce bandwidth and the network connection at this university became slow. Then the computer centre requested the professor's assistance with the investigation. The professor was the just person he gave his confession and showed his record of "open ports" from some top universities. Besides, the professor had a proof for his motive in the form of a manuscript of an article.

The university's computer centre was once concerned with his act. But after the professor understood all he had done, the professor told him two points:

1. Stop his experiment immediately even if it was useful for me;
2. Let him ensure no actual access to any computer and investigation would concluded, and no worry.

He was fortunate as his experiments were understood by a professor who knew both computer science and law; and the computer centre was so wise, nice and kind that they didn't take the matter for granted as a crime or a war. He was not an offender, nor a warrior.

Many others were not as lucky as him. In approximately the same season, a student at another university was found guilty of using a computer doing similar things as his, accessing several computers in that country, revising data or even programs in them. That student's case was investigated by criminal police and he made real trouble with his computer. He might have not given as perfect an explanation about his work as the scholar had about mine. Thus he might well be regarded as a cyber offender, or a cyber warrior, or even a cyber spy. A long judicial procedure and investigation were waiting for him, enough to interrupt his study.

In the scholar's opinion, the sophistication and scale of so-called cyber warfare can undoubtedly realized by one single person with one single computer, not to say many users might make spontaneous reaction to a certain event. They do not need any coordination; but the timing of the event might act as a "coordinator". Sometimes, two separate attacks might just coincided in time, target or origin, as millions of users might be online at any moment, and that two or more users with similar interest or sentiment act simultaneously does not sound so fictional.

But media might misconnect some individual people, individual events, individual targets or individual origins with each other and create some mysteries of cyber warfare. Stories from one source read imaginative; from two sources read justified; and from three or more sources read as true as facts. Once something is labeled cyber warfare, other things can be similarly labeled as well. Then the discourse of "cyber warfare" will detect its expression in real life. Cyber warfare industry will create quite good business opportunities for interested players all across the society.

Conclusion

There has been a growing concern over cyber warfare have in recent decades. War-oriented writer usually exploited such serious and expensive terms as cyber war, information war, and electronic war to spread their impetuous and cheap ideas. More and more parties are involved in spreading the discourse about the potential threat of cyber warfare. All of them seem to benefit from an enlarged version of an imagination. A new industry is growing up, exploiting new terminologies such as cyber warfare, electronic war, and information warfare. Examples given in this essay are only tip of the iceberg. Here, I want to borrow from Morozov (2009b), saying that,

“The age of cyber-warfare has arrived. That, at any rate, is the message we are now hearing from a broad range of journalists, policy analysts, and government officials.”

References

Derene, Glenn. How Vulnerable is U.S. Infrastructure to a Major Cyber Attack? Popular Mechanics, April 2009.

Economist. 2007. Cyberwarfare Is Becoming Scarier, May 24.

Eriksson, E. Anders. 1999. The Non-proliferation Review, Spring-Summer, pp. 57-64.

Gardham, Duncan. 2009. Al-Qaeda, China and Russia 'pose cyber war threat to Britain', warns Lord West, June 25, 2009. Retrieved July 17, 2009, from <http://www.telegraph.co.uk/news/newstopics/politics/lawandorder/5634820/Al-Qaeda-China-and-Russia-pose-cyber-war-threat-to-Britain-warns-Lord-West.html>

Morozov, Evgeny. 2009a. 10 Easy Steps to Writing the Scariest Cyber Warfare Article Ever, April 11, 2009. Retrieved July 17, 2009 from http://neteffect.foreignpolicy.com/posts/2009/04/11/writing_the_scariest_article_about_cyberwarfare_in_10_easy_steps

Morozov, Evgeny. 2009b. Cyber-Scare: The Exaggerated Fears over Digital Warfare. Boston Review, July/August 2009.

Poulsen, Kevin. 2007. Estonia “Cyberwar” Wasn’t. Retrieved July 17, 2009, from http://www.wired.com/threatlevel/2007/06/estonia_cyberwa/

Ranum, Marcus J. The Problem with Cyber War (Video), DojoSec Monthly Briefings, March 2009. Retrieved July 17, 2009, from [http://securitytube.net/Cyber-War-is-Bullshit-\(Dojosec\)-video.aspx](http://securitytube.net/Cyber-War-is-Bullshit-(Dojosec)-video.aspx)

Smith, George. 2003. Iraqi Cyberwar: an Ageless Joke. Retrieved July 17, 2009, from <http://www.securityfocus.com/columnists/147>

Smith, George. 2007. The Clowns of Cyberwar: Rediscovering electronic Pearl Harbor, always handy fodder for the lazy opinion page editor, October 8, 2007. Retrieved July 17, 2009, from <http://www.dickdestiny.com/blog/2007/10/clowns-of-cyberwar-rediscovering.html>

UK Office of Cyber Security and UK Cyber Security Operation Centre. 2009. Cyber Security Strategy of the United Kingdom, safety, security and resilience in cyber space, June 2009.

Regulation of Cyberspace: Chinese Law on Cybersecurity and Cybercrime

Abstract

Since the advent of the network era, different countries adopted different stance on maintaining social order in cyberspace, either soft, strong, or in a medium of the way. In China, as in some other countries in the same group, a tough approach has been taken from the beginning. The purpose of this article is, by studying a series of legal actions against cybercrime, to explore into the Chinese model of regulation on cyberspace. In order to exercise control over the Internet, China has implemented statutory laws and administrative regulations revolving activity criminalizing, content filtering and user monitoring so as to maintain security and stability at both community and state levels. A tight legal and regulatory network has gradually weaved through recruitment of cyber police, investment on security technology, regulations on communications enterprises, and surveillance over users. Regardless of critics, this model was proved to have the merits of effectiveness in the specific socio-legal context in a short term.

Keywords: Chinese law, cybercrime, criminalization, regulation on cyberspace

1. Introduction

Recent two decades witnessed a swift transforming human and social landscape due to the pervasive use of digital networks, which connect individuals, institutions, businesses and agencies spreading over the world. The growing convenience for creating, depositing, processing, transmitting, and retrieving of information increased the quantity of data in both static and dynamic processes, improved virtual

communication, developed social networks, and at the same time, risks, threats and dangers have also been unignorable problems.

Naturally, it was not strange that information systems in the background of Chinese history had been regarded as a modern instrument in an ancient territory. In fact, many countries were confronted with similar challenge at the dawn of the information age, when they were perplexed for how to benefit from the pervasive use of information systems while avoiding negative political and legal impact of unmonitored users, uncensored information, unchecked communications, uncontrolled activities and unsolicited visits. Such potentialities were also eroding footstones of the Chinese Great Wall.

Additionally, migration of criminal phenomena into information systems-facilitated cyberspace has attracted increasing attention due to its high pace of expansion (Li 1992; Li 1993; Li 2003a; Li 2003b; Li 2008; Li 2009). The 1997 Penal Law of China (which was usually translated as Criminal Law but Penal Law should be more exact translation) provided fundamental criteria and guidelines for convicting and sentencing cybercriminals. With assistance of a series of other statutory laws and administrative regulations, a legal and regulatory system has been taking shape to suppress the spread of cybercrime of multiple forms, the so-called new century's pestilence, in cyberspace. The explosion of new and pertinent laws and regulations over the past two decades reflected society's concerns on the ancient phenomenon in a modernized context, and efforts to wrestle with it. Yet, it remained uncertain whether the current approach to deter and redress cybercrime would prove to be successful.

In the following sections, this article will review the process of establishing the legal framework on cybersecurity and cybercrime in China, examine the features of Chinese laws and regulations tackling cybercrime, and analyze the policy for preventing cybercrime through control over cyberspace in China. The article will also analyze the subject, the means, the mechanism and the main purpose of control over cyberspace, with empirical review of its actual effects and defects.

2. Criminalization and penalization of cybercrime

The “chance encounter” of communist China based on its ancient land and people with the information network had multiple potentialities of changing the politico-social order, which were unexpected and unprepared events in the late 20th century. According to official statistics, to the end of 2014, the number of Internet users in China reached 649 million and the number of mobile Internet users reached 557 million (China Internet Network Information Centre 2015). It was estimated that there are already 721 million users in 2016, more than half of Chinese population (Internetlivestats.com 2016). The use of mobile instant message apps had grown steadily, attracting 91.2% of the mobile Internet users (China Internet Network Information Centre 2015). Cybersecurity accidents and cybercriminal cases are both increasing stubbornly (The National Computer Network Emergency Response Technical Team/Coordination Centre of China 2014). Crimes and criminals come in all varieties on the Internet, ranging from the catastrophic to the merely annoying (Icove and co-workers 1995). Therefore, defined broadly, the term “cybercrime” could reasonably cover an extensive variety of criminal offences, activities, or issues. In China, the term has been the same from the beginning, pronounced as “jisuanji fanzui” (computer crime). Now, the term more frequently used is “wangluo fanzui” (network crime). Nevertheless, there has never been an official term for it. The crimes promulgated in the Penal Law of China are more complicated, because the Penal Law itself did not give simplified names to any offences.

In Chinese academic world, a variety of definitions were introduced from the Western countries, or some new definitions were proposed, including those either in broad sense or in strict sense. Most of these definitions have been derived from the Western countries, with their books and articles translated into Chinese and published in China. The subsequent study witnessed some rational thinking about the issue, and some definitions came into being which possessed the Chinese style. The definitions introduced to China and proposed by Chinese scholars had profound academic significance before the amendment of the Penal Law in 1997. The following sections

will comprehensively review these terms and definitions through taxonomic analysis.

2.1. Three layers of cybercrime conception

Cybercrime, as a conception with broad interpretation, has been defined at three different levels in China's laws:

At the first level, computer crime was prescribed by Articles 285, 286, 286-1, 287, 287-1 and 287-2 of the 1997 Penal Law in Chapter VI, "Crimes of Disrupting the Order of Social Administration" (1997 Penal Law; 2015 Penal Law Amendment IX). According to the 1997 Penal Law, computer crime is a crime in which computer information systems are targets of the crime. But the 2015 Amendment IX expanded criminalization and penalization to network service providers' failure to perform their network security obligations resulting in serious consequences, knowingly providing technical or material support to online criminals, using networks to teach or facilitate criminal behaviour, as well as setting up or utilizing a wireless station (stand) without authorization, or utilizing a wireless frequency without authorization, to disturb wireless communication order. Considering criminalization and penalization of cybercrime at this level, the criminalizing scope was too narrow to cover the practical illegal acts related to computer, and necessitated enlargement in the legislation.

At the second level, it can be stated that the definition of computer crime in the Penal Law is of only nominal meaning. In effect, cybercrime in China covers extraordinarily wide range of offences. When discussing the problem of cybercrime, we should use the term in the criminological sense but not limited to that in the Penal Law. As Li (1992) pointed out that, the traditional Penal Law of China could be interpreted and adjusted to punish cybercriminal offences according to different existing clauses. Actually, it has been usual practice in China as well as in some other countries where there were no existing law dealing with computer crime but computer crimes occurred. It was very rare that perpetrators were left unpunished when offences were detected and convictions were established. Of course, this did not neglect the fact that many existing cases were never detected, and many detected

cases were never punished due to substantive law and procedural law obstacles.

At the third level, there were still some more categories clustered in academic research. Computer-related crimes could exist in every chapter of special part of the Penal Law, from offences against national security to those against economy, from offences against person to those against property, etc. (Li 1992) Moreover, as it was concluded that a clear difference between law and policy did not even exist in China, while policy could be similarly effective as those formally enacted law (Clarke 1999). This was determined by the methodology of Chinese mode of thinking, which was on the same basis as the system of guilty analogy that was repealed in 1997.

All the three levels of meanings of cybercrime were similarly important when we studied Chinese laws, regulations and policy pertinent to cybercrime. It is necessary to indicate that some researchers eccentrically asserted that, “China does not seem to possess any written law or code specifically outlining its computer crime statutes...trials are held by the force of military law...” (Kim 1997) Unfortunately, this claim was based on a noticeable misunderstanding of the present status of Chinese legal system, which has been developing rapidly and in fact closely following the track that many industrialized countries went along (Li 2014; Li 2015). Military offences, which were once prescribed by a single act, which paralleled the Penal Law, were shrunk into one chapter of the whole Penal Law in 1997. Before that, according to our analysis, most computer crimes could have been penalized according to many pertinent clauses of the Penal Law, or in rare cases, penalized according to military offences.

Obviously, criminal punishments on all offences were harsh in China. Criminal punishment in China ranged from fixed-term imprisonment to death penalty, decided by the types of crimes that were committed. Concerning cybercrime, the Supreme People’s Court (2001) ruled that capital punishment might be applied to those who provided state secret to foreign individuals or institutions via the networks and cause particularly serious harm.

2.2. System of cybercriminal Law

Computer crime emerged in China in mid-1980s and was punished within the previously existing legal framework. According to Chinese law, computer was only an object or a tool of various crimes, which could cover counter-revolutionary offence, offence against public security, offence against personal rights and democratic rights, offence against property, offence against social management order, and offence of malfeasance. Different situations, where computer played different roles and caused different harmful results to different targets, can be criminalized and penalized according to provisions on different offences. The old law has since challenged and developed under pressure of the pervasion of the information systems and the emergence of crimes connected with the cyberspace.

Specific regulation on cybercrime started in 1994 when the State Council promulgated the Ordinance on Security Protection of Computer Information System (State Council Decree No. 147, 18 February 1994). The Ordinance prescribed legal liability for five types of activities: (1) violating security ranking protection systems of computer information systems, and threatening the computer information systems; (2) violating the registration system of computer information systems international networking; (3) not reporting cases happened in the computer information systems according to the prescribed time; (4) refusing to improve after receive the notice from the public security agency requiring improving the security situation; and (5) other acts threatening the computer information systems (Ordinance on Security Protection of Computer Information System, Chapter 4).

These acts were punishable by public security for admonition or rectification upon stopping the computer (Ibid, Article 20). If the conduct violated the public security management, it would be punishable according to Regulations on Public Security Management; if the conduct constituted an offence, it should be held criminally liable according to the then effective 1979 Penal Law (Ibid, Article 24), in which apparently no such an offence like a computer crime was ever mentioned.

Problems involved in such provisions could be analyzed from two aspects:

In case the conduct constituted an offence, it was punishable according to Penal

Law. However, the Penal Law of the time did not provide relevant punishment for any offence involving computer system or computer networks (Penal Law of People's Republic of China, 1979). The provision of "when the conduct constitutes an offence, it should be held criminally liable" was in want of immediate legal sources, but was possible to be solved by the potentiality of the existing Chinese law dogmatism through analogical interpretation of existing offences in the Penal Law by the Supreme Court (but note, conviction through analogy was formally repealed in 1997), or to be solved by a quick amendment of it.

Another problem was that subjects of liability, i.e. those perpetrators who would be held liable for the offence, were not clearly and reasonably defined. For example, in the provision on the offence of "not reporting cases happened in the computer information systems according to the prescribed time" (Ordinance on Security Protection of Computer Information System, Article 24 (3)) obviously imposed liability on the victimized party. That is to say, the users were both the target of the offence and the subject of liability.

However, the interpretation function of the Chinese law was so strong that any legal loopholes could be filled through interpreting and applying the existing law. Consequently, hacking could be a conduct punishable according to the 1979 Penal Law, where provisions were very vague, the openness was strong enough to cover new offences that were initially not defined clearly. However, investigation and conviction of computer crime were treated very carefully due to concerns on the legal gaps, because innovative, enlightened and progressive theoretical, legislative and judicial blueprints would soon change the whole system.

The amendment of Penal law in 1997 added two clauses on computer crimes, one was illegal intrusion into computer information systems in Article 285 and the other, destruction of computer information systems in Article 286. The Penal Law was promulgated at the beginning of the year, when use of the Internet was expanded extraordinarily fast. As soon as some computer crimes were criminalized by the new Penal Law, newer problems on the Internet posed newer challenges instantaneously. As a reaction to new problems, in 2000, the Standing Committee of the National

People's Congress promulgated a comprehensive law to maintain the Internet security, Decision on Maintaining Internet Security, which was the only law on Internet security passed by the legislature, besides the 1997 Penal law. It has been 20 years when the 9th Amendment of the Penal Law formally extended criminalization in 2014, by adding three new Articles 286(1), 287 (1) and 287 (2) to cover offences committed by network service providers of failure to perform their network security obligations resulting in serious consequences of causing NSP security failures, providing technical support to criminals, and spreading criminal information.

(i) Criminalizing intrusion into computer information systems

The offence of intrusion into computer information systems was the conduct of intrusion into computer information systems of national affairs, national defence construction, and of the field of advance science and technology, violating national provision (The Penal Law, Article 285). In a document ratified by the Minstry of Public Security in 1997, Management Measures of Security Protection of International Networking of Computer Information Networks, the conduct of entering the computer information networks or using the computer information network resources without permission was listed as one of the activities threatening computer information networks security and hence prohibited (Management Measures of Security Protection of International Networking of Computer Information Networks, Article 6 (1)). In provisions regulating the Internet online services business locations, managing units and online users were prohibited from illegal intruding into computer information systems or destructing function, data and applied programs of computer information systems and threatening security of information networks (Ordinance on Management of Internet Online Services Business Place, Article 15 (2)). Obviously, these provisions demonstrated the necessity for extending the prohibition of hacking activities to the extent that Article 285 of the Penal Law could not cover, and added the prohibition of using resources of computer information networks without permission. Acts violating law, administrative regulations, without permission, entering into computer information networks or using resources of computer information networks, should be given warning by the public security agency; when

those acts involving illegal income, illegal income should be confiscated; and individual or unit should be combined with a certain sum of fine. In case the situation was grave, when interruption of online services and rectification beyond shutting down the computers were caused, combined punishment should be imposed for an imprisonment not longer than six months. If necessary, the previous institutions that granted the certificate or license might be proposed to withdraw the managing license or abrogate the qualification of online services; if the conduct constituted the conduct violating public security management, it should be punishable according to the Ordinance on Public Security Management Sanctions; if the conduct constituted a crime, penal liability should be imposed according to the Penal Law (Management Measures of Security Protection of International Networking of Computer Information Networks, Article 20).

The Decision on Maintaining Internet Security restated that if the conduct of intrusion into computer information systems of national affairs, construction of national defence, and advanced science and technology constituted a crime, penal liability should be imposed according to the Penal Law (Decision on Maintaining Internet Security, Article 1 (2)). However, the Decision would not punish general hacking activities, which targeted computer information systems not belonging to China, or targeted computer information systems not belonging to the above three specific categories.

(ii) Criminalizing information-related or content-related offences

In China, as in some other countries in the world, freedom of speech had specific implications and was evaluated with specific criteria. Free speech in one country might be banned in another country. Therefore, online contents were thought to be posing great challenge to state security and social stability according to the official concerns of China. Due to the significance of information or contents themselves, this made up the single most important category of cybercrime in Chinese law, which could also be used to demonstrate how laws and regulations were affected and alarmed by the Internet, and how laws and regulations would deal with new challenges posed by the Internet.

The first provisions concerning the online contents were implemented in the Temporary Provisions on Management of International Networking of Computer Information Networks of 1996 (promulgated by State Council Decree No. 195 on 1 February 1996, amended on 20 May 1997). The Provisions required that units and individuals that were engaged in Internet business should abide by related law and administrative regulations, strictly enforce security and secrecy systems, must not engage in transgress and criminal activities of threatening state security and revealing state secret and other activities with the Internet, must not create, retrieve, duplicate and spread information that disturbs the social security and obscene and erotic and other information (Article 13). The Provisions provided that, acts violating these provisions, and violating other laws and administrative regulations as well, should be punished according to related laws and administrative regulations; if constituting a crime, penal liability should be imposed according to the Penal Law (Article 15).

According to China's law, the Provisions presented the determination of the Chinese government to punish the criminal activities on the Internet. In the meantime, it was obvious that emphasis of the Provisions was on control of Internet contents, particularly, three categories of information, which was related to state security, public security, and which was obscene and erotic information, were prohibited. It implied the possibility of punishing the activities of creating and spreading computer virus, instructing hacking knowledge, as well as creating and spreading information impeding public security. More seriously, simply to browse certain information was also prohibited according to these Provisions.

In Management Measures of Security Protection of International Networking of Computer Information Networks, prohibition on online contents was expanded to nine aspects, primarily covering state security, social stability and personality and reputation, but no reflection to economic interests. Abuse of the Internet was first of all regarded as a potential political threat, while the influence on economy was so far not considered. The Management Measure prescribed that no unit or individual might use the Internet to create, replicate, retrieve, or transmit the following kinds of information (Article 5): (1) inciting to resist or undermine the implementation of

constitution, laws, or administrative regulations; (2) inciting to overthrow the government or socialist system; (3) inciting to split the country, threatening national unification; (4) inciting hatred or discrimination among nationalities or harming the unity of nationalities; (5) making falsehoods or distorting the truth, spreading rumours, destroying order of society; (6) promoting feudal superstitions, sexually suggestive material, gambling, violence, murder, terrorism or inciting other criminal activities; (7) openly insulting other persons or distorting the truth to defame other persons; (8) damaging the reputation of state organs; (9) other activities breaching Constitution, laws or administrative regulations.

Since 2000, prohibitions of online contents were re-grouped, however, still into nine categories. The most significant change was addition of prohibition of “breaching state religious policy, advocating teachings of evil cults.” Prohibition of online contents was further strengthened and the coverage was broadened. In a series of governmental documents implemented afterwards, nine new prohibitions were specially underlined. These governmental documents involved provisions on Internet services of different departments and in different fields. In September 2000, the State Council passed simultaneously Ordinance on Telecommunications (passed on 31st Standing Meeting of State Council on 20 September 2000, and promulgated by State Council Decree No. 291 on 25 September 2000) and Management Measures on Internet Information Services (passed on 31st Standing Meeting of State Council on 20 September 2000, and promulgated by State Council Decree No. 292 on 25 September 2000). The Ordinance provided that no organization and individual might create, duplicate, publish and spread messages containing these contents via the telecommunications networks (Ordinance on Telecommunications, Article 57). The Management Measures provided that providers of Internet information services must not create, duplicate, publish and spread messages containing these contents (Management Measures on Internet Information Services, Article 15). Ministry of Information Industry’s Management Provisions on Internet Electronic Bulletin Services (November 2000) provided that no one might publish messages containing one of these contents in the electronic bulletin service system (Article 9). Ministry of

Information Industry's Temporary Provisions on Management of Internet Website Engaged in Business of News Publication (November 2000) provided that news published on Internet websites must not contain these contents (Article 13). Ministry of Education's Notice on Printing and Distributing "Management Provisions on Electronic Bulletin Services of Colleges and Universities Computer Networks" (Jiao She Zheng (2001) No. 10 on 21 October 2001) provided that users of bulletin board system websites should abide by provisions by pertinent laws and regulations, and must not create, duplicate, publish and spread messages containing these contents (Article 13). Management Measures on Internet Domain Names (Ministry of Information Industry, Management Measures on Internet Domain Names, entering into force on 30 September 2002) provided that no organizations or individuals might register and use domain names containing these contents (Article 19).

The nine new prohibitions covered the following categories: (1) information that breaches basic principles of the Constitution; (2) information that endangers national security, divulges state secrets, subverts the government, or undermines national unity; (3) information that is detrimental to the honour and interests of the state; (4) information that instigates ethnic hatred or ethnic discrimination, or that undermines national unity; (5) information that undermines the state's policy towards religions or that advocates the teachings of evil cults or that promotes feudalistic and superstitious beliefs; (6) information that disseminates rumours, disturbs social order, or undermines social stability; (7) information that spreads pornography or other salacious materials; promotes gambling, violence, homicide, or terrorism; or instigates crimes; (8) information that insults or slanders other people, or infringes upon other people's legitimate rights and interests; or (9) other information prohibited by laws or administrative regulations.

In sum, some governmental documents pertinent to regulation on cyberspace supplemented the nine new prohibitions. Subsequently, ten prohibitions took a shape with the addition of one more prohibition, i.e., prohibition on "threatening social morality or national excellent cultural tradition", listed before the previous ninth prohibition, elaborated by such documents as Ordinance on Management of Internet

Online Services Business Place (promulgated by State Council Decree No. 363, entering into force on 15 November 2002), which provided that no management units of Internet online services business place and online consumers might use the Internet online services business place to create, download, duplicate, retrieve, publish, spread or use messages containing these contents by other means (Article 14); Article 17 of the General Office of Press and Publications and Ministry of Information Industry's Temporary Provisions on Internet Publication Management (entering into force on 1 August 2002) provided that Internet publications must not publish these contents (Article 17); Ministry of Culture's Temporary Provisions on Internet Culture Management (entering into force on 1 July 2003) provided that Internet culture units must not provide cultural products containing these contents (Ibid, Article 17). From these laws and regulations, a clear picture on how the Internet affected Chinese law and how Chinese law dealt with the Internet was painted.

In Management Measures on Video and Audio Programs Spread on Internet and other Information Networks issued by General Bureau of State Broadcasting and Television (entering into force on 10 February 2003), these prohibitions were further extended to 12 categories by adding false information and overseas programs received and recorded from the networks or overseas media as programs forbidden to spread through information networks (Article 19). However, shortly afterwards, these measures were repealed by new document of the same name issued in July 2004, entering into force in October of the same year, when these two new categories were removed and only ten prohibitions left.

As an important law criminalizing certain (regarded as harmful) activities on the Internet, the prohibitions in the Decision on Maintaining Internet Security could be summarized into three categories nine aspects. The law provided that if any one, who committed one of these acts and constituted a crime, should be held liable according to the Penal Law. Here is a panorama of the legal system containing criminalized activities that mainly involved online information and contents alone:

- (1) Maintaining state security and social stability
 - (a) The acts of exploiting the Internet to disseminate rumours, slander or

publish, to spread other harmful information, to instigate to subvert state regime, to overthrow socialist system, or instigate to split the state, to undermine the state unity (Decision on Maintaining Internet Security, Article 2 (2)), was indictable as the offence of instigating to subvert state regime (Punishable according to the provisions of Articles 105 (2), 106, 56 and 113 of Penal Law) and offence of instigating to split the state (Punishable according to the provisions of Articles 103 (2), 106, 56 and 113 of Penal Law).

(b) The conduct of stealing, divulging state secret, intelligence or military secret (Decision on Maintaining Internet Security, Article (2)), might constitute offence of stealing, spying out, purchasing, illegally providing state secret, intelligence (Penal Law, Articles 111, 113, and 56), offence of illegal obtaining of secret (Ibid, Article 282 (1)), offence of illegal possessing of state secret (Ibid, Article 282 (2)), offence of internationally divulging state secret (Ibid, Article 398), offence of negligently divulging state secret (Ibid, Article 398), offence of illegally obtaining of military secret (Ibid, Article 431 (1)), offence of stealing, spying out, purchasing, illegally providing military secret (Ibid, Article 431 (2)), offence of intentionally divulging military secret (Ibid, Article 432), and offence of negligently divulging military secret (Ibid, Article 432).

(2) Information that instigated ethnic hatred or ethnic discrimination, or that undermined national unity, or violated national customs and habits

(c) The conduct of exploiting the Internet to instigate ethnic hatred, ethnic discrimination, undermine ethnic solidarity (Decision on Maintaining Internet Security, Article 2 (3)), constituted the offence of instigating ethnic hatred or ethnic discrimination (Penal Law, Article 249).

(d) The acts of exploiting the Internet to organize evil cult organizations, making contact with members of evil cult organizations, undermining the enactment of state law and administrative regulations (Decision on Maintaining Internet Security, Article 2 (4)), constituted the offence of organizing or exploiting superstitious sects and secret societies or evil cult organizations, or exploiting superstitions to undermine the enactment of law (Penal Law, Article 300 (1)), and the offence of

organizing or exploiting superstitious sects and secret societies or evil cult organizations, or exploiting superstitions to cause death (Ibid, Article 300 (2)).

(3) Maintaining socialist market economic order and social management order

(e) The acts of exploiting the Internet to marketing false and interior products, or falsely propagate products or services (Decision on Maintaining Internet Security, Article 3 (1)), constituted the offence of producing or marketing false and interior products (Penal Law, Articles 140-150), and offence of false advertising (Ibid, Articles 222 and 231).

(f) The conduct of exploiting the Internet to damage others' commercial credit or merchandise reputation (Decision on Maintaining Internet Security, Article 3 (2)) constituted the offence of damaging commercial credit or merchandise reputation (Penal Law, Articles 221 and 231).

(g) The conduct of exploiting the Internet to infringe others' intellectual property (Decision on Maintaining Internet Security, Article 3 (3)) might be punished according to the offences of infringing trademark right, copyright, patent right or business secret (Penal Law, Articles 213-220).

(h) The conduct of exploiting the Internet to fabricate and spread false information that influences the transaction of securities or futures, or other information that disordered the financial order (Decision on Maintaining Internet Security, Article 3 (4)), constituted the offence of manoeuvring transaction price of securities or futures (Penal Law, Article 181).

(i) The conduct of setting up obscene website or webpage, providing link services of obscene website, or spreading obscene books and periodicals, film, phonotape and videotape or pictures (Decision on Maintaining Internet Security, Article 3 (5)), might constitute the offence of creating, duplicating, publishing, selling, or spreading obscene goods to seeking interests (Penal Law, Articles 363 (1) and 366), and the offence of spreading obscene goods (Ibid, Article 364 (1)).

(4) Protecting personal rights, property rights and other legal rights of individuals, corporations and other organizations

(j) Insulting or fabricating facts to libel others with the Internet (Decision on

Maintaining Internet Security, Article 4 (1)) constituted offence of insult and libel. Except those gravely endanger the social order and state interests, these offences are disposed only upon charge of the victim (Penal Law, Article 246).

The Temporary Provisions on Internet Publication Management prescribed that no Internet publication contents primarily targeting the juveniles might contain contents that induced juveniles to imitate activities breaching social morality or activities of transgress and crime, as well as the contents of terror, cruelty or other contents that were harmful to juvenile health of body and mind (Temporary Provisions on Internet Publication Management, Article 18). If the Internet publishing institutions published or transmitted these prohibited contents, however, no criminal liability was prescribed. The illegal income should be confiscated by related authorities. Different sum of fine could also be imposed according to the sum of illegal dealing (Ibid, Article 27).

(iii) Criminalizing the offence of interfering the functioning of computer information systems

The conduct of violating the state provision, deleting, modifying, adding, or interfering the functioning of computer information systems, and causing the abnormal functioning of computer information systems, with the grave after-effect, was punishable by imprisonment of less than five years or penal servitude; with specially grave after-effect, was punishable by imprisonment of no less than five years (Penal Law, Article 286 (1)). Decision on Maintaining Internet Security incorporated the acts of violating state provisions, interrupting computer networks or communications services without authorization, and causing the computer networks or communications systems unable to function normally, into one offence (Decision on Maintaining Internet Security, Article 1 (3)).

(iv) Criminalizing the offence of destructing data and programs

The conduct of violating state provisions, deleting, modifying or adding to the data and applied programs deposited, processed, or transmitted in the computer information systems, with grave after-effect, was punishable by imprisonment of less than five years or penal servitude; with specially grave after-effect, was punishable

by imprisonment of no less than five years (Penal Law, Article 286 (2)).

According to Management Measures of Security Protection of International Networking of Computer Information Networks, and Ordinance on Telecommunications, the above activities were punishable by warning, fine, shutting down business no more than six months; in case involving grave situation, no more than six months of disconnection and rectification could be imposed. If necessary, the previous institution that issued the certificate, or the institution responsible for examination and approval, could be recommended to withdraw the management license or cancel the qualification of connection; if the conduct constituted a conduct violating public security management, it was punishable according to Ordinance on Public Security Management Sanctions; if the conduct constituted crime, the perpetrator should be held criminally liable according to law (Management Measures of Security Protection of International Networking of Computer Information Networks, Article 20).

(v) Criminalizing the offence of creating or spreading computer virus

The Management Measures on Computer Virus Prevention (passed by Ministry of Public Security on 30 March 2000) prohibited any unit or individual to create (ibid, Article 5), spread computer virus (ibid, Article 6), and publish false computer viruses epidemic situation to society (ibid, Article 7). Activities of spreading computer virus included: intentional inputting computer virus, threatening security of computer information systems; providing others with files, software, or media containing computer virus; selling, renting, or presenting media containing computer virus; other activities of spreading computer virus (ibid, Article 6). The Management Measures of Security Protection of International Networking of Computer Information Networks prohibited intentional creation or spreading computer virus or other destructive programs (Article 6 (4)). Ordinance on Management of Internet Online Services Business Place also prohibited management unit of business place of Internet online services and online consumers to intentionally create or spread computer and other destructive programs, and threaten the security of information networks (Article 15 (1)).

Ordinance on Security Protection of Computer Information System, also prescribed relevant sanction to such activities (Articles 24 and 20). The Penal Law prescribed that intentional creation or spreading computer virus and other destructive programs, influencing the normal functioning of computer system, with grave after-effect, was punishable according to the provision on the offence of destructing computer information systems (Penal Law, Article 286 (2)). In Decision on Maintaining Internet Security, a similar provision was restated (Article 1 (2)). In publishing false epidemic situation of computer virus to society, different sums of fine could be imposed to both unit and individual perpetrators (Management Measures on Computer Virus Prevention, Article 17).

(vi) Criminalizing the offence committed by exploiting computer and the Internet

According to Article 287 of Penal Law, in case where other offences were committed involving the factor of a computer, the acts were punishable according to the pertinent provisions. The other articles of the Penal Law did not contain the term “computer”, but some offences could be committed with the help of a computer. Due to validity of Article 287, such activities have been naturally covered by the Penal Law.

The Penal Law prescribed that if a computer was exploited to commit financial fraud, theft, embezzlement, defalcation, theft of state secret or other offences, the perpetrator was punishable according to related provisions of the Penal Law (Article 287). Decision on Maintaining Internet Security prohibited theft, fraud, and racketeering exploiting the Internet (Article 4 (3)).

The coverage of Management Measures of Security Protection of International Networking of Computer Information Networks was even broader. No unit and individual might exploit the Internet to threaten state security, divulge state secret, infringe state, social, collective interests and citizens’ legal interests or engage in activities of transgress and crime (Article 4). The conduct violating this provision was punishable according to laws and statutes (ibid, Article 22).

Exploiting the Internet to commit other offences not explicitly listed in

Articles 1-4 of Decision on Maintaining Internet Security, could also be held criminally liable according to pertinent provisions of the Penal Law (Decision on Maintaining Internet Security, Article 5). This article reserved the spirit of Article 287 of the Penal Law, further extending the application scope to offences committed exploiting the Internet (besides a computer) as an instrumentality.

(vii) **Criminalizing the offence of infringing freedom of communications**

The users' freedom and secret of communications were protected by law. No unit or individual might violate the provision of law, exploiting the Internet to infringe users' freedom and secret of communications (Management Measures of Security Protection of International Networking of Computer Information Networks, Article 7). The conduct violating the provisions of law, exploiting the Internet to infringe the users' freedom and secret of communications was punishable according to laws and statutes (ibid, Article 22).

Decision on Maintaining Internet Security criminalized the conduct of illegal interception, modification and deletion of others' electronic mail or other data and information, infringing the citizen's freedom and secret of communications (Decision on Maintaining Internet Security, Article 4 (2)).

These activities were punishable according to pertinent provisions in the Penal Law (Penal Law, Article 252). The electronic mail and other data were brought into the field of communications. The Internet was the means, only by which this offence was committed.

(viii) **Criminalizing the conduct of network service providers failing to perform their obligations**

In 2014, the 9th Amendment of the Penal Law added a new provision holding network service providers liable for their failure to perform their network security obligations resulting in serious consequences. If network service providers did not perform information network security management duties as provided by law or administrative regulations, and upon being ordered by the oversight and management department to adopt rectification measures still do not make corrections, they were punishable by up to three years imprisonment, short-term detention or controlled

release, and/or a fine. One of the following situations must be met for the conviction: (a) where it resulted in the transmission of a large volume of unlawful information; (b) where it resulted in disclosure or user information causing serious consequences; (c) where it results in the destruction of evidence in a criminal case and the circumstances are serious; or (d) there are other serious circumstances (Penal Law, Article 286-1).

(ix) Criminalizing the conduct of using information networks to commit other offences

Use of information networks to commit any of the following conduct, where the circumstances are serious, is punishable by up to three years imprisonment or short-term detention, and/or a fine: (a) setting up a website or mail list used to conduct fraud, transmit criminal methods, make or sell prohibited or controlled items, or other illegal activities; (b) publishing illegal or criminal information related to producing or selling drugs, guns, obscene items or other prohibited or controlled items; and (c) publishing information for committing fraud or other illegal or criminal activities (Penal Law, Article 287-1).

(x) Criminalizing the conduct of spreading criminal information

Clearly knowing that others are using information networks to perpetrate crimes, and providing them with technical support such as internet access, server hosting, web storage, or communications transfer, or providing help such as in advertising and promotions or paying bills, where circumstances are serious, is sentenced by up to three years imprisonment or short-term detention and/or a fine (Penal Law, Article 287-2).

(xi) Criminalizing other conducts threatening computer information networks security

Management Measures of Security Protection of International Networking of Computer Information Networks prescribed that violating laws and administrative regulations, any other conducts threatening the computer information networks security, should be imposed a warning, fine, or shutting-down of business for no more than six months; in grave situation, no more than six months of disconnection

and rectification might be imposed. If necessary, proposal could be made for the previous institution that issued the certificate, or the institution examined and approved, to withdraw the management license or cancel the qualification of networking; if the conduct constituted a conduct violating public security management, it was punishable according to Ordinance on Public Security Management Sanctions; if the conduct constituted crime, the perpetrator should be held criminally liable according to law (Article 6 (5) and 20). Here, the term “law” that could impose criminal penalties included but was not limited to the Penal Law.

3. Control over the Internet

From the very beginning, China has been making efforts to create a giant domestic intranet while barring out the global Internet in order to control the network by central government (Franda 2002, p. 187). The goals of China’s operations against online activities, which were regarded as harmful, were more concentrated on maintaining state security than any other aspects. As long as cybersecurity was concerned in the Chinese context, it has frequently been understood as a critical part of state security. The authority tended to view the single access to information that was different from political interests as potential threats to stability, and thus showed no tolerance. Thus, freedom of speech bears different meaning from the notion in the Western world. As introduced in previous parts of the article, dozens of laws, rules, and regulations have been installed to normalize the use of the information network services. Traditional official agencies have been granted new functions, while brand new agencies and institutions have been established to exercise control over the Internet.

In regulating information network services, particularly online speech and business information caused great anxiety from enterprises and human rights organizations.

3.1. Central players: cyber police

In order to exercise control over the information networks, i.e. to control users and Internet service providers (ISPs), many traditional agencies and new agencies found their way into the new domain and coordinated in the new battlefield. One of them, state security agency, a less publicized intelligence agency, has been said to play a critical role in fight against conducts threatening state security. Within public security agencies, cyber police teams, armed with knowledge and skills of information technology, were established. From publicly available information, state security agency was relatively a small entity, and of course was not the only and the primary agency to exercise control over conducts on the Internet. Comparatively, cyber police forces were by far the strongest among all the agencies with the task of tackling malicious online conducts. The actual control over the Internet went beyond the imagination of people from outside world. Users should always go online with great care for fearing that they would be shadowed by the police, listed in the blacklist, and secretly detained and investigated, or even publicly arrested. Those who actually violated laws and regulations might face punishment of different severities.

On the other hand, actual controllability of online conducts has been proved to be weak. Early surveillance of computer networks in China was hampered by such obstacles as insufficient cyber police force, out-dated computer protection equipment imported in the 1980s and 1990, and slow development of computer protection products. Once lagging behind in science and technology of computing, today's China has changed dramatically in recent two decades. With the growth of cyber police in number, power, knowledge and skills, techniques, experience, more and more websites and messages might be monitored and blocked, and more and more users might be investigated and punished. Of course, the factor that the government might become more tolerant of some of the online conducts and messages has also changed more or less the nature and feature of laws, regulations and particularly policies.

3.2. Major means: blockade of the information network

Blockade was a term used in International law to denote the action of the outside world to block a certain state. But the Chinese blockade of the information network did not mean the same. On the contrary, it meant that China blocked itself from the outside information network. The original idea was to create a “Chinternet”, the information network with Chinese characteristics. Once it proved to be impossible, China turned to fence the information network with such things as those walls built around private yards and between neighbours in old times to function as let-in and let-out switch. The term “blockade” of information networks covered a wide scope of meaning, from limiting access to banning certain contents. Blockade was not the only effect that illegal contents might cause, but breach of which was also the reason for further legal actions. Merely breach of the blockade might already incur punishments at various levels, which might take many forms such as being deprived of the permit to use the network, or fines, confiscation of equipments as well as prison terms.

The most efficient way of exercising control over online activities was through control over access to the network. In China in late 1990s and early 2000s, cyber café was a very popular business, facilitated with the then newest generations of computer and fastest network connections. These cyber cafés could become the focus of law enforcement because most of the online conducts and messages would take place there. As a method of blockade, close-down of net cafés was warmly welcomed by the police forces, which could benefit by ways of transferring equipments under their control, or in many cases by taking bribes from owners of the businesses. It depended on how the state policy was: if the policy permitted such businesses to continue, a sum of bribery would ensure that the business would continue; or if the policy prohibited such businesses some day, the business owners might lose anything due to breach of the new policy. Many possibilities existed, but one of the most interesting requirements on business owners was to keep a list of their customers, who were registered in the list by showing their identification cards. Once there were suspected offences, the list should be submitted to authorities so as to make it more convenient to investigate the cases. However, thousands of net cafes throughout China were

forced to close down throughout 2000s. In addition, authorities required users of online services to buy specific personalized identity cards, enabling close monitoring the websites that they surfed. A user must register her/his personal details, such as name, age and address, which would be kept in a central database. Control over the online services proved to be costly, a fact that the authorities have already realised. However, it seemed to be identified as the most effective method and all attempts were made to be practised.

From those laws and regulations cited in previous sections, it was obvious that it was not a secret that the government made great efforts to regulate online contents. Cyber police were responsible for sniffing out and blocking access to those proxy servers located outside China. A broad range of new filtering techniques were introduced, including filtering a list of keywords, which were adjusted over time according to development of detailed political and social situations. Some online forums and bulletin board system (BBS) have practised corresponding self-control mechanism. For example, it was almost impossible to register a user account not to say to publish a message in Qiangguo Forum especially from a foreign computer.

What worried the authorities was that the WWW, email, BBS, instant messages (IMs) and social network services (SNSs) have been used by political dissidents, exiles from minority territories, as well as others, to circulate information and to publicize their cause or to seek supports for online petitions. To deal with all these activities, China sought to cooperate with global giant enterprises of online commerce to control the flow of information imported to or exported from China over the networks. This kind of cooperation occurred in both routine filtration and occasional case investigation. In order to survive in the specific online environment in China, many online business companies adopted strategies in subjection to the official requirements, refusal of which might lead to banned access or termination of business within Chinese border. For example, retreat of Google from Chinese market in 2010 could partly be attributed to strict requirements that Google could not meet.

Some BBSs and forums were strictly limited access within China. In some cyber cafés, the keepers also screened their machines from browsing foreign websites,

including free email service providers in a relatively flexible way. Upon negotiation with the managers, they would authorize the use of free web-based email systems. Owners of some cyber cafés formulated two standards of charge, the lower one for services of limited surfing, and the higher one for services of unlimited browsing, due to different levels of risks they might face. In China, it was possible to retrieve adult websites, but it was strictly not possible to retrieve political websites with contents that were identified as threatening communist rule and socialist system. Keepers of cyber cafés had also a stake in serving their customers.

3.3. Core of the mechanism: joint liability

Concerning the responsibility mechanism of control over the online services, joint liability has been established, both macroscopically and microscopically, both in central and local governments. The responsibility and liability bound all pertinent governmental ministries and basis units. If officials were regarded as negligent when malicious conduct took place with grave results, they could face criminal or administrative liabilities. These responsibility and liability were regulated in almost all the laws and regulations concerning control over information networks.

Article 8 of Regulations on Protection of State Secrets in Computer Information Systems on the Internet stipulated the principle that responsibility was borne by the person who placed it on the Internet. It was the basis for punishment of the conduct of revealing state secrets on the Internet. However, this did not exempt the obligation of individual ISPs to monitor the Internet. Under Article 10, ISPs, BBSs, chat rooms or newsgroup organizers were required to set up their own management mechanisms to assist ensuring that their users transmit no state secret on the Internet.

Nonetheless, this kind of joint liability was similar to personal liability in cases of someone breaching the birth control policy. However, if the criminal fled, the liability would be transferred to certain scapegoats. Chapter IX of the Penal Law of China provided the liability for neglecting duty for government functionaries, under which officials must be careful in exercising their duties, and under the pressure of

which they must also closely monitor a school of other players involved in online services, regardless of their identities as providers or users.

3.4. Purpose of regulation: state stability

What posed a great challenge to the artificial political system was that more people than ever used the information networks to propagate their “anti-revolutionary”, “liberalist”, and “separatist” ideas, made complaints and express their discontent. “Chinese people” was not a term that tallied with the Chinese territory. All over the world, there were Chinese who owned various national, political and religious views inherited from each historical period. Although policies of China have taken a big stride toward democracy and freedom within the past four decades when it carried out reform and openness to the outside world, various views still could not be in harmony with the official stance. In particular, Chinese government has never publicly admitted that it made any of its policy under any outside pressure or in accommodation to the views of any dissident groups. That was an issue of “face”, which meant no compromise under pressure.

Free information was not limited to that was useful to commerce and technology. However, in the context of China, regulation on the Internet was designed to eliminate harmful information while reserving useful information. People from some other countries worried that this kind of regulation would have negative effect on protection of human rights and development of economy, just contrary to the spirit of the Internet.

In fact, besides the action against information breaching state political interests, China also contributed to maintain the security of information systems. Most of the prosecuted cases have been criminal offences involving embezzlement, fraud, hacking and defacing, and virus spreading. Therefore, by emphasizing that China concerned and thus did a lot in maintaining state stability, it did not reject all the efforts of the Chinese authorities in combating cybercrime in recent years, when more and more perpetrators, who were involved in both domestic and international

offences, have actually been investigated by Chinese cyber police.

3.5. Negative implications of the regulation

People always had scruples when they went online, worrying that they might retrieve web pages with contents that the government might impose a ban. Laws and regulations provided only rough principles on identifying contents that were banned. Users had to judge by themselves whether or not the retrieved contents were prohibited. For example, if users opened an online forum full of messages with various opinions, they must judge at the first sight which category the web pages belonged to: separatism, terrorism, dissidents, or national secret. The users could only skip those web pages, close them with great care, and leave the machine with great panic. This kind of side psychological effect brought about by strict regulation frightened many users.

4. Critics on substantive law system on cybercrime

Chinese laws on cybercrime covered a wide range of conducts and implement various penalties. However, there were still many loopholes in these revisions. The main problems were: overlap of provisions, missing of referred regulations and laws, narrow criminalization, narrow constituents, and laggard penalties. The following sections present these problems in detail.

The first aspect involved overlap of provisions. Article 286 of the Penal Law provided different activities. The first paragraph criminalized the conduct of destructing computer information systems. The second paragraph outlawed the conduct of destructing system data and applied programs. The third paragraph prohibited the conduct of intentionally creating and spreading viruses. The first two paragraphs were termed from the aspect of objects of the conduct, while the latter one was termed from the aspect of form of the conduct. By comparing these three paragraphs, we could find that they were overlapped. Generally, creating and

spreading computer viruses could result in abnormal operation of the systems, and could also destruct data and applied programs in the systems. At present, most of the abnormal operation of the computer systems and the destruction of data and applied programs were committed by the use of computer viruses. This resulted in the simultaneous application of the two paragraphs. Scholars proposed that a solution to this problem is to divide conducts covered by this Article into two different offences, one was direct destruction of computer systems, and the other, destruction with computer viruses.

The second aspect mentioned the legal gap formed in referring to other laws and regulations. Compared with European Convention on Cybercrime (CETS No.185), Chinese laws and regulations on cybercrime in fact fully criminalized the activities covered by the Convention. These laws and regulations outlawed various cybercrime and gave appropriate punishments, including public security management punishments, administrative punishment, penalty and measures limiting the qualification of holding a post. Problems were that when the nature and situation of these criminalized activities were grave, they should be punished by penal law. When the penal law was not perfect (of course no law was perfect, by default, conducts not prohibited by law were permitted), the provision “holding criminally liable according to law” became invalid. Possible problem was that a lighter cybercrime (transgress) would be imposed public security management punishment or administrative punishment, while some of the graver cybercrime (crime) could be held “criminally liable” “according to law,” due to missing of such laws.

The third aspect was concerning the narrow scope of criminalization. Huang and Chen (2005) pointed out that Article 285 of the Penal Law limited objects of the offence to computer information systems of national affairs, construction of national defence, or belonging to the field of top science and technology. With development of the Internet, security of other computer information systems has also been necessary to enjoy protection. Therefore, the protection scope should be extended (Huang and Chen 2005).

The fourth aspect criticized narrow legal constituents. According to the Penal

Law, subject of computer crime was limited to natural persons. The corporate liability should be added (Huang and Chen 2005). According to Article 17 (2), a person who was older than 14 years old but younger than 16 years old, was only criminally liable for eight kinds of severe offences: intentional homicide, intentional injury resulting in grave bodily harm and death, forcible rape, robbery, sales of drug, arson, explosion, and spread poison. Many of the perpetrators of cybercrime were younger than 16 years old. Some scholars proposed that the scope of subjects of cybercrime should be extended, that is to say, applying a lower liable age. In 2015, when the ninth Amendment of the Penal Law was issued, this problem was partially solved, because a unit now could be held liable for cybercrimes according to the revised clauses.

Finally, the laggard penalty provision was also a focus of criticism. Huang and Chen (2005) also pointed out that the Articles 285 and 286 of Penal Law provided the imprisonment as the only punishment for offences against information systems, without possibility of imposing fine and disqualification. In many other countries, all of the three types of punishments were possible to be imposed. Considering the deterrent effect, they proposed that Chinese law should also be revised to add more types of punishments (Huang and Chen 2005), which were partially realised by adoption of the ninth Amendment of the Penal Law.

5. Conclusion

In control over the online services, China took a series of actions characterized by content filtering and activity monitoring, for the purpose of maintaining state stability as well as cyber security. A close network was formed to prevent and deter cybercrime by recruitment of cyber police, investment on security technology, imposing requirements on the e-commercial enterprises, and surveillance on users.

These countermeasures that China adopted to fight against cybercrime had commonness with other countries. First of all, criminalisation has been a significant way to incorporate the actions into the legal framework. Notwithstanding the

difference with regard to the social system, legal framework in China was developing with a fast step. The penal law was not an exception. Promulgation of the 1997 revision and more subsequent amendments of the Penal Law and a series of regulations helped form a systematic legal framework against cybercrime. Second, Chinese law covered most of the cybercrime offences that have been criminalized in industrialised countries. Therefore, if there was the necessity of international coordination between China and other countries, substantive law basis has been to some extent prepared. Furthermore, Chinese control over the Internet was not without precedents. In practice, many control measures adopted in China were similar to those in the United States and some European countries, despite that there were still differences based on socio-legal contexts.

Certainly, control mode of China had its speciality. Firstly, focuses of legal actions in China were characterised by emphasizing the maintenance of state stability and social order. The core of all focuses was on online speech that breached state regulation. Anxiety of the authorities was that absolute free speech would erode the foundation of state politics, for which criminalisation of content-related offences took an unparalleled coverage than many other countries. Secondly, Chinese legal system was more flexible than many other countries. The forms (or “sources” in jurisprudence) of laws were diversified, including the penal code, special statutes, legislative and judicial interpretations, and administrative regulations, all being integrative parts in criminalizing the pertinent conducts. Thirdly, combat and prevention were designed to be combined with each other. The deterrence system did not only play a role on preventing potential perpetrators from committing cybercrimes but also play a role in detecting occurred offences. Fourthly, strike-hard strategy was used occasionally. Strike-hard strategy has been used in China since early 1980s to clamp down rising waves of crime. At present, this strategy was also used in fighting against various specific crimes, including offences endangering public order, offences of illegal publications, offences related to pornographic materials, etc. Generally, various computer- and network-related offences were fought together with content-related offences during strike-hard actions.

References

China Internet Network Information Center. (2015). *35th Statistical Survey Report on the Internet Development in China*, Beijing: China Internet Network Information Center.

Clarke, D. (1999). Private Enforcement of Intellectual Property Rights in China, in *Intellectual Property Rights in China: Evolving Business and Legal Frameworks*, Volume 10, Number 2, National Bureau of Research Analysis.

Franda, M. (2002). *Launching Into Cyberspace: Internet Development and Politics in Five World Regions*, London: Lynne Rienner Publishers.

Huang, Z. and Chen, X. (2005). The Defects of Criminal Law Regulation and Theoretical Reaction to Computer Crime, *Jianghai Xuekan*, Issue 3, pp. 112-118.

Internetlivestats.com. 2016. China Internet Users. Retrieved 27 April, 2016 from <http://www.internetlivestats.com/internet-users/china/>.

Kim, M. W. (1997). How Countries Handle Computer Crime, *Ethics and Law on the Electronic Frontier*. Fall 1997

Li, X. (1992). A Study on the Application of Criminal Law to Computer Crime, *China University of Political Science and Law Graduate Law Review*.

Li, X. (1993). On Several Issues of Computer Crime. Master Thesis. Beijing, China: China University of Political Science and Law.

Li, X. (2003a). Thinking about Cybercrime in China. *Asian and Comparative Law*, 1 (1), pp. 52–55.

Li, X. (2003b). Criminalization and Regulation of Cybercrime in China. *Asian and Comparative Law*, 1 (2), pp. 3–17.

Li, X. (2008). *Cybercrime and Deterrence: Networking Legal Systems in the Networked Information Society*. Turku, Finland: University of Turku.

Li, X. (2009). *Social Order in Cyberspace*. Hyderabad, India: ICFAI University Press.

Li, X. (2014). *Zhongguo Falv Zhidu Daolun* (An Introduction to Chinese Legal

System). Turku, Finland: Informyth.

Li, X. (2015). Chinese Legal System: A Way Forward. In X. Li (ed., 2015). Selected Readings in Chinese Legal System. Turku, Finland: Informyth. pp. xvii-xx.

Li, X. (ed., 2015). Selected Readings in Chinese Legal System. Turku, Finland: Informyth.

The National Computer Network Emergency Response Technical Team/Coordination Center of China (known as CNCERT or CNCERT/CC). (2014). *Report on China Internet Network Security 2013*. Beijing: CNCERT/CC

Home	Table of Contents	Titles & Subject Index	Authors Index
----------------------	-----------------------------------	--	-------------------------------

International Actions against Cybercrime: Networking Legal Systems in the Networked Crime Scene

[Xingan Li](#)

Faculty of Law, University of Turku, 20014 Turun Yliopisto, Finland. E-mail: xingan.li (at) yahoo.com

Received August 28, 2007; Accepted September 26, 2007

Abstract

This article reviews the international impetus of criminal law reform in combating cybercrime. This article classifies actions of international harmonization into professional, regional, multinational and global actions, summarizes the major concerns of these actions, and concludes the influence of the Convention on Cybercrime on state and international levels of legal countermeasure. The article also points out the limitations of the previous actions and anticipates the United Nations to play a more important role.

Keywords

Cybercrime; Legal system; International harmonization

Introduction

Traditionally, crime and punishment are largely local, regional, or national. Today, many differences confronting us are associated with the transnational character of cybercrimes. It is therefore important to have international legal instruments ready to serve anti-crime efforts.

This article looks at international harmonizing efforts to fortify the legal battle against cybercrime, categorizing the actions into four aspects: professional law-enforcement efforts, regional efforts, multi-national efforts, and global international efforts. Subsequently, the article also categorizes the international actions according to the subject-matters into additional aspects, including the promotion of security awareness at both international and national levels, the harmonization of legislation, coordination and cooperation between law-enforcement agencies, and direct anti-cybercrime actions. The article will also examine the nations' attitudes toward the Convention on Cybercrime. Based on the analysis, the article will briefly evaluate the effectiveness of previous attempt at international harmonization.

From domestic legislation to international harmonization

People usually are impressed by the illusory overlap between Internet space and

international space. Notwithstanding the fact that information systems are linking continents, islands, residents and communities into a giant virtual network, states and areas preserve their traditional sovereignty. [McConnell International](#)'s metaphor (2000, p. 8) said that: "In the networked world, no island is an island." At this turning point, the globally connected Internet has made cybercrime a trans-border problem. The "international dimension" ([Wasik](#), 1991, pp. 187-201), "trans-national dimension" ([Sofaer & Goodman](#), 2005) or "global dimension" ([Grabosky](#), 2004, pp. 146-157) of cybercrime is universally perceived. While law is always territory-based, the tool, the scene, the target, and the subject of cybercrime are all boundary-independent. Domestic measures will certainly be of critical importance but not sufficient for meeting this worldwide challenge. International coordination and cooperation are necessary in fighting offences commonly prohibited by every country.

Many international organizations have been making efforts to harmonize actions within their forums. Many authors have also been pursuing research on international harmonization from different standpoints and for different goals; for example, [Sieber](#) (1996, 1998), United Nations Crime and Justice Information Network ([UNCJIN](#), 1999), [Police Commissioners' Conference Electronic Crime Working Party](#) (2000), [Sofaer et al.](#) (2000), [Putnam and Elliott](#) (2001), [Schjølberg & Hubbard](#) (2005), and so on. Although information about the basic facts of international harmonization that these research studies deal with is the same, different knowledge can be drawn from different thinking. For the purpose of convenient summarization within this article, we categorize the international harmonization actions into the following groups: professional organizations, regional organizations, multi-national organizations, and global organizations. Many other valuable international actions have simply not been considered due to the limit of this study (it is hardly possible to assume that studies on cybercrime can cover all useful international actions of international organizations at all levels).

Professional efforts of International Criminal Police Organization (Interpol)

Many international organizations qualify for professional organizations, because their goals and activities are focused on certain specific issues; these organizations include Interpol, the International Telecommunications Union, etc. However, professional efforts here primarily mean substantial actions in the field of cybersecurity protection and cybercrime prevention. Although some other organizations also greatly contribute to coordinating cybersecurity protection, their emphasis is not necessarily on the law. By this standard, this section only analyzes the actions of the International Criminal Police Organization (Interpol).¹

As an international law-enforcement organization with 184 members, Interpol started to tackle computer crime very early, coordinating law-enforcement agencies and legislations, in regard to which Interpol made efforts to improve counter-cybercrime capacity at the international level. A 1981 survey of members on cybercriminal law recognized dilemmas in application of existing legislation ([Schjølberg & Tingrett](#), 2004). Based on the recognition of the legal gaps between countries, and gaps between the legal framework and criminal phenomena, Interpol expanded its task to both law enforcement and legal harmonization.

Currently, there are four working parties within the framework of Interpol, comprising African, American, Asia-South Pacific and European Working Parties on Information Technology Crime. Besides these groups, a Steering Committee for Information Technology Crime was established in order to harmonize the different

regional working-party initiatives.² Considering the already-harmonized legislation as the prerequisite for the coordinated law enforcement, the African Working Party agreed upon "the project on legislation and comparative law existing in the Africa with a view to having more African states co-signing and/or ratifying the Council of Europe Cybercrime Convention."³ Apparently, legal harmonization is one of Interpol's important tasks in working towards an effective law-enforcement environment.

In regard to law enforcement, Interpol has provided a technical guidance in cybercrime detection, investigation and evidence collection. The Interpol Information Technology Crime Investigation Manual was compiled by the European Working Party on Information Technology Crime.⁴ Compared with the substantive and procedural law harmonization of today's Convention on Cybercrime, the Manual developed a technological law-enforcement model to improve the efficiency of combating cybercrime.

Along with efforts in law enforcement on cybercrime, Interpol also takes distinct actions to prevent cybercrime, cooperating with credit-card companies to combat payment fraud by building a database on Interpol's web site ([Police Commissioners' Conference Electronic Crime Working Party](#), 2000, p. 64). As one of the necessary cooperation projects at the international level of law-enforcement, cybercrime and other trans-border crimes are specially dealt with by Interpol in gathering and sharing information. In addition, Interpol is making efforts to establish a network to for harvesting information relating to activities on the Internet.⁵

Regional efforts

There are many regional international organizations, with a narrow or broad coverage of states, more or less making efforts to maintain cybersecurity and harmonize international measures to combat cybercrime. This section will introduce only four of these organizations, which have taken typical actions in combating cybercrime.

(i) The Asia-Pacific Economic Cooperation (APEC)

In the Asia-Pacific region, the APEC coordinates its 21 member economies to promote cybersecurity and to tackle the risks brought about by cybercrime ([APEC](#), 2003). The APEC has conducted a capacity-building project on cybercrime for member economies in relation to legal structures and investigative abilities, where the advanced APEC economies support other member-economies in training legislative and investigative personnel.⁶

After the 9/11 attacks on the U. S., the APEC Leaders issued a Statement on Counter-Terrorism, condemning terrorist attacks and considering it urgent to reinforce collaboration at different layers to fight against terrorism. The Leaders called for reinforcing APEC activities to protect critical infrastructure.⁷

The Telecommunications and Information Ministers of the APEC economies issued the Statement on the Security of Information and Communications Infrastructures and a Programme of Action in 2002,⁸ supporting measures taken by members to fight against misuse of information. The Senior Officials' Meeting has made a recommendation which designates six areas that can serve as the foundation for the APEC's endeavor for cybercrime prevention, comprising legal development, information sharing and cooperation, security and technical guidelines, public awareness, training and education, and wireless security.⁹ The Ministers and Leaders

of APEC have made a commitment to "endeavour to enact a comprehensive set of laws relating to cybersecurity and cybercrime that are consistent with the provisions of international legal instruments, including the UN General Assembly Resolution 55/63 and Convention on Cybercrime by October 2003."¹⁰

In response to this call from the leaders, a survey of laws was carried out and a summary was made of the responses from member economies received in 2003 (see [E-Security Task Group](#), 2003). The economies proposed corresponding projects in information-security task groups. For example, the U.S. proposed a project in the E-Security Task Group of the Telecommunications and Information Working Group. The first phase of this project was a meeting of cybercrime experts from around the region. The meeting was held from 21-25 July, 2003 in Bangkok, Thailand, and was attended by over 120 delegates from 17 economies. The objectives of the meeting were to assist the economies to develop the necessary legal frameworks; to promote the development of law-enforcement capacity; and to strengthen cooperation between private and public sectors in addressing the threat of cybercrime.¹¹ In the conference, the experts present agreed that every economy needed a legal framework including one for substantive and procedural law, and for the law and policies of inter-economies cooperation. They confirmed the role of international instruments, particularly the Convention on Cybercrime. They also emphasized jurisdictional cooperation, law-enforcement construction, and the capacity building of the investigators.¹²

In 2005, The sixth APEC Ministerial Meeting on the Telecommunications and Information Industry passed the Lima Declaration, "encouraging all economies to study the Convention on Cybercrime (2001) and to endeavor to enact a comprehensive set of laws relating to cybersecurity and cybercrime that are consistent with international legal instruments, including UN General Assembly Resolution 55/63 (2000) and the Convention on Cybercrime (2001)."¹³ However, due to the great difference between member economies within the APEC, the development toward unified legal instruments has not been too satisfactory. Although some economies have claimed that their laws have been completely consistent with the Convention, and some other economies were taking actions to implement provisions similar to the Convention, many other countries have quite different legal systems or have no law criminalizing cybercrime.

Efforts are still to be made in the forum of the APEC to address cybercrime. The U.S. proposed the Judge and Prosecutor Cybercrime Capacity Building Project in 2006 in order to develop a curriculum devised by government and private sector experts; to translate the curriculum into domestic languages; and to train the trainer (judges and prosecutors).¹⁴

(ii) The Council of Europe (COE)

The Council of Europe has been working to tackle rising international anxiety over the risks brought about by the automatic processing of personal data since the early 1980s.¹⁵ In 1981, the Council of Europe implemented the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (ETS No. 108, 26 January 1981), which was revised according to the Amendment to Convention ETS No. 108 Allowing the European Community to Accede, 15 June 1999, and the Additional Protocol to Convention ETS No. 108 on Supervisory Authorities and Trans-border Data Flows, 8 June 2000. The Convention recognized the desirability "to extend the safeguards for everyone's rights and fundamental freedoms, and in particular the right to the respect for privacy, taking account of the

increasing flow across frontiers of personal data undergoing automatic processing," and the necessity "to reconcile the fundamental values of the respect to privacy and the free flow of information between peoples" (Preamble). The Convention covers the protection of personal data in both the public and private sectors.

Chapter II of the Convention established basic principles for data protection, one of which is data security (Article 7), covering the prohibition of accidental or unauthorized access, alteration and dissemination.

The expert committee appointed in 1985 published Recommendations of 1989 and 1995, addressing the issues of substantive laws and procedural law in this area respectively (See Recommendation No. R. (95) 13).

Recommendation R. No. (89) 9 recognized the importance of an adequate and quick response to the new challenge of computer-related crime, which often has a trans-border character, and recommended the governments to consider the Report on Computer-Related Crime drawn up by the European Committee on Crime Problems.

Then there is Recommendation No. (95) 13 Concerning Problems of Criminal Procedure Law Connected with Information Technology. The Recommendation recognized that information systems may also be used for committing criminal offences, evidence of criminal offences may be stored and transferred by these systems, while the criminal procedure law of member states often do not provide for appropriate powers to search and collect evidence in these systems during a criminal investigation. The appendix to the Recommendation lays down the principles for criminal procedure laws on search and seize, technical surveillance, obligations to co-operate with the investigating authorities, electronic evidence, use of encryption in research, statistics and training, and international cooperation.

In 1997, the Council of Europe began drafting the Convention on Cybercrime, which was open for signature in 2001 and took effect in 2004.¹⁶ In 2003, the Additional Protocol to the Convention on Cybercrime Concerning the Criminalization of Acts of a Racist and Xenophobic Nature Committed Through Computer System (ETS NO. 189) was implemented. The Convention addresses substantive law, procedural law, jurisdiction, and international law in the field of cybercrime. The Convention is a historic landmark in the combat against cybercrime. It is expected that the Convention will have a deep impact on the legal reform relating to cybercrime in its 46 member states and one candidate state.

In the 2004 Conference on Cybercrime, the Council of Europe called for "wide and rapid" access to and "effective implementation" of the Convention on Cybercrime, raising awareness in the highest political level, and encouraging cooperation between public and private sectors.¹⁷

In the 2005 Conference on Cybercrime, the Council of Europe expressed concern about the fast-increasing threats and serious social and economic results of cybercrime including terrorist activity on the Internet, noting that most cybercrime is international cybercrime, recognized the need for effective and compatible laws and tools to enable efficient cooperation to combat cybercrime, calling upon public and private cooperation, and encouraging access to the Convention on Cybercrime.¹⁸

In 2006, the Council of Europe launched a Project against Cybercrime, intended to grant assistance to the development of national legislation in line with the provision of the Convention, training of judges, prosecutors and law-enforcement officers, and training of criminal justice officials and 24/5 contact points in international

cooperation.

(iii) The European Union

The EU took a series of actions to tackle cybercrime through impelling a coordinated law enforcement and legal harmonization policy. Civil liberty has also been a focus in the anti-cybercrime field.

In 1995, the European Parliament and the Council endorsed Directive 95/46/EC of 24 October 1995 on the protection of Individuals with regard to the Processing of Personal Data and on the Movement of Such Data. Section VIII of the Directive specifically deals with confidentiality and security of processing of personal data. The Directive applied to protection of natural persons (Article 2(a)). The scope of the Directive was limited to the processing of personal data entirely or partially by automatic means (Article 3-1). The Directive required that appropriate technical and organizational measures have to be implemented to protect personal data against illegal destruction, alteration, access and other illegal forms of processing (Article 17-1).

The Directive required the Member States to provide administrative and judicial remedies for the victim (Article 22), and provided for the compensation liability of (Article 23) and sanctions on (Article 24) the transgressor.

In 1997, the European Parliament and the Council endorsed Directive 97/66/EC of 15 December 1997 concerning the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector. The Directive was aimed at furthering the protection implemented in Directive 95/46/EC, and providing for the harmonization of the member states' provision to attain an equivalent level of protection (Article 1-1). The Directive extended the protection of legitimate interests to legal persons (Article 1-2).

The application scope of the Directive was limited to the processing of personal data relating to the provision of publicly available telecommunications services in the public telecommunications networks; particularly via the ISDN (Integrated Services Digital Network), and public digital mobile networks (Article 3-1). As the Directive 95/46/EC is concerned with automatic processing systems, Directive 97/66/EC has emphasized the linkage with the telecommunications network. The Directive provides requirements directly targeted at the service providers (but not member states) "to take appropriate technical and organizational measures to safeguard the security of its services." (Article 4-1). The Directive requires the Member States to implement the regulations ensuring the confidentiality of communications, prohibiting listening, tapping, storage or other kinds of interception or surveillance of communications by unauthorized natural and legal persons (Article 5). The Directive limited unsolicited communications (Article 12), which covers automatic calling systems or facsimile machines, but not e-mails.

On 27 November 2001, a plenary session took place in Brussels of the EU Forum on Cybercrime, organized by the EC,¹⁹ and where the primary discussion was about the retention of traffic data ([EU Forum on Cybercrime](#), 2001).

In April 2002, the [Commission of the European Communities](#) presented a proposal for a Council Framework Decision on Attacks against information systems, and this proposal constitutes the case of the Decision of 24 February 2005.²⁰ The Framework Decision criminalized the offences of illegal access to information systems (Article 2), illegal system interference (Article 3), illegal data interference (Article 4), and

instigation, aiding and abetting of these offences or attempt at them (Article 5). The Framework Decision only dealt with attacks through unauthorized access to or interference with information systems or data. According to the Decision, illegal access can only be constituted when the illegal activities are targeted intentionally against an "information system with specific protection measures in place and [the attacks] must be for economic gain." (Article 2)

The Commission further considered the future possibility of "specific protection measures" (Proposal for a Council Framework Decision on Attacks against information systems) to broadband networks, saying that, "it is necessary that criminal law covers unauthorized access to their systems even though there may not be adequate technical protection for their systems." (ibid.) Thus, concerning the interference with information systems, it is constituted by serious "hindering" or "interrupting" of the functioning of information systems by "inputting, transmitting, damaging, deleting, deteriorating, altering, suppressing or rendering inaccessible computer data" (Article 3).

This Framework Decision does not specify penalties for illegal access to information systems and instigation, aiding and abetting and attempting of these offences, but requires member states to take the necessary measures to ensure that they are punishable by effective, proportional and dissuasive criminal penalties (Framework Decision, Article 6.1). The Decision specifies the penalties for illegal system interference and illegal data interference as punishable by criminal penalties to a maximum of at least one to three years of imprisonment (Article 6.2). As for the "aggravating circumstances", the criminal draws a maximum of at least two to five years imprisonment (Article 7.1). These aggravating circumstances include an organized attack, and an attack that has "caused serious damages or has affected essential interests" (Article 7.2). Criminal organization is defined as a "structured association, established over a period of time, of two or more persons, acting in a concerted manner with a view to committing offences."²¹

It is worth noting that the matters mentioned in the Framework Decision can also be found in the Convention on Cybercrime.²² After revision of the legislation required by the Convention, the national law (of Finland) will also meet the demand of the Framework Decision.²³ Today, comprised of 27 member states and three candidate countries, the EU remains active in addressing cybercrime.

(iv) The Organization of American States (OAS)

As other regional organizations, the Organization of American States (OAS) with 35 member states is also highly concerned about the issue of cybercrime. Through its forum for the Ministers of Justice or of the Ministers or Attorneys General of the Americas (REMJA), the OAS has long recognized the central role that a sound legal framework plays in combating cybercrime and protecting the Internet. Such recognition has prompted the REMJA to recommend the creation of the Group of Governmental Experts on Cybercrime (The Group of Experts) in March 1999.²⁴ The Group of Experts has been devoted to analyzing cybercrimes, to inspecting the domestic cybercrime law, and to finding ways of cooperating in the Inter-American system of combating cybercrime. The Group of Experts has held four meetings.²⁵

The Meeting of the Ministers of Justice or of the Ministers or Attorneys General of the Americas (REMJA III)²⁶ has urged member states to take steps to endorse cybercrime law; harmonize cybercrime laws to make international cooperation possible. The Meeting of the Ministers of Justice or of the Ministers or Attorneys

General of the Americas (REMJA V) ²⁷ has recommended that member states evaluate the advisability of implementing the principles of the Convention on Cybercrime, and consider the possibility of acceding to that Convention.

In 2004, the Fourth Plenary Session of the Organization of American States General Assembly passed the resolution on "Adoption of a Comprehensive Inter-American Strategy to Combat Threats to Cybersecurity: A Multidimensional and Multidisciplinary Approach to Creating a Culture of Cybersecurity," proposing that "An effective cybersecurity strategy must recognize that the security of the network of information systems that comprise the Internet requires a partnership between government and industry."²⁸

Multi-national efforts

Unlike professional organizations that are limited to a more specific field of concern, and unlike regional organizations that are limited to a more specific location of states, the multi-national international organizations care for affairs of a broader range and take actions in a broader territorial environment. This section recounts the efforts of three of the multi-national organizations.

(i) The Commonwealth of Nations

The Commonwealth of Nations took a direct and timely action in the harmonizing laws of its member states. In October 2002, the Commonwealth Secretariat prepared the "Model Law on Computer and Computer Related Crime" ([Bourne](#), 2002, p. 17). Within the Commonwealth's 53 member countries, the "Model Law" has had a wide influence on domestic legislation. Through this model law, the Convention on Cybercrime has become one of the legislative choices in substantive criminal law, covering the offences of illegal access, interfering with data, interfering with computer systems, illegal interception of data, illegal data, and child pornography.

Compared with the Convention on Cybercrime, the Model Law expanded criminal liability - so as to include reckless liability- for the offences of interfering with data, interfering with computer systems, and using illegal devices. The Model Law also covered the problem of dual criminality by stating that the act applied to an act done or an omission made by a national of a state outside its territory, if the person's conduct would also constitute an offence under a law of the country where the offence was committed. This may lead to prosecution or extradition based on dual criminality, but not extradition as it is provided in the Convention on Cybercrime.²⁹

Some of the member countries of the Commonwealth have made efforts to draft domestic law according to the model law, such as Bahamas and St. Lucia.³⁰ In Barbados, Belize, and Guyana, the Model Law is being considered as a guide to the enactment of similar legislation.³¹ However, in many other countries of the Commonwealth, there is still no special legislation for cybercrime.³²

Besides impelling legislation within the forum, another focus of the Commonwealth is on mutual assistance in law enforcement between Commonwealth member states and between Commonwealth member states and non-Commonwealth states. In the 2005 Meeting of Commonwealth Law Ministers and Senior Officials, the Expert Working Group proposed 10 recommendations for member states to adopt suitable measures for improving domestic law enforcement and trans-national assistance, and encouraged member states to sign, ratify, accede to and implement the Convention on Cybercrime as a basis for mutual legal assistance between Commonwealth member

states and non-Commonwealth states.³³

(ii) The Group of Eight (G8)

Since the mid-1990s, the Group of Eight (G8) has created working groups and issued a series of communiqués from the leaders and actions plans from justice ministers. At the [Halifax Summit](#) 1995, the Group of Seven recognized "that ultimate success requires all governments to provide for effective measures to prevent the laundering of proceeds from serious crimes, to implement commitments in the fight against trans-national organized crime."³⁴ The group released 40-point set of "recommendations to combat Trans-national Organized Crime efficiently" at the G7/P8 Lyon Summit. The recommendations urged the states to increase the level of criminalization, prosecution, investigation, and international cooperation, while acknowledging in their entirety human-rights protection.³⁵

At the [Denver Summit](#) 1997, the Group of Eight proposed to strengthen their efforts to realize the Lyon recommendations, by concentrating on punishing high-tech criminals, and promoting the governments' technical and legal abilities to react to trans-territorial computer crimes.³⁶ The Group of Eight Meeting of the Justice and Interior Ministers of December 1997 responded to the increased international movement of criminals, organized crime, and terrorists and their use of the ICT.³⁷ Ministers noted, in a Statement of Principles Concerning Electronic Crime, that, while criminal legislation was a national responsibility, the character of the information networks obstructed countries from operating traditional power over this problem. Domestic legislations have to be complemented by international cooperation to criminalize the abuse of the networks and harmonize the investigative action.³⁸

At the subsequent summits, the Group of Eight repeatedly expressed their concern about cybercriminality. At the Okinawa Summit, the Okinawa Charter on Global Information Society adopted the principle of international collaboration and harmonization of cybercrime. "In order to maximize the social and economic benefits of the information society", the Group of Eight agreed on principles and approaches for the protection of privacy, the free flow of information, and the security of transactions.³⁹ The Charter recognized that the security of the information society necessitated coordinated action and effective policy responses.⁴⁰

(iii) The Organization for Economic Cooperation and Development (OECD)

With its 30 member countries, the [OECD](#) addressed computer security for several decades. In 1983, an expert committee was appointed by the OECD to discuss computer crime phenomena and criminal-law reform ([Schjolberg & Hubbard](#), 2005). Offences against confidentiality, integrity or availability listed in the 1985 OECD document included unauthorized access, damage to computer data or computer programmes, computer sabotage, unauthorized interception, and computer espionage.⁴¹ In December 1999, the OECD officially approved the *Guidelines for Consumer Protection in the Context of Electronic Commerce* ([Department of Justice](#), 2000, p. 27), representing member states' consensus in the area of consumer protection for e-commerce: consumers should be protected in e-commerce not less than the protection they enjoyed within traditional commerce ([Department of Justice](#), 2000, p. 27). The OECD adopted Guidelines for the Security of Information Systems and Networks in July 2002, calling on member governments to "establish a heightened priority for security planning and management", and to "promote a culture of security among all participants as a means of protecting information systems and

networks" ([OECD](#), 2002a, Part I).

The guidelines established nine principles, including awareness, responsibility, response, ethics, democracy, risk assessment, security design and implementation, security management, and reassessment ([OECD](#), 2002a, Part III). Because of the nature of the guidelines and the distance from the legal actions, practical endeavors were left to the member countries to make.

Global international efforts by the United Nations (UN)

There are numerous global organizations. Nevertheless, the UN is capable of being identified as the only global organization that forms a forum of its 191 member states with fuller functions. Compared with professional organizations, the UN does not limit its activities to certain domains. Compared with regional organizations, the UN does not limit its activities to certain states (in the field of cybersecurity protection and cybercrime prevention). The actions of the UN have unique advantages in coordinating international positions.

In 1985, General Assembly Resolution 40/71 of 11 December called upon governments and international organizations to take action in conformity with the recommendation of the commission on the legal value of computer records of 1985, in order to ensure legal security in the background of the broadest possible use of information processing in international transactions.^{[42](#)}

In 1990, the General Assembly of the UN adopted the Guidelines Concerning Computerized Personal Data Files. It proposed to take appropriate measures to protect the files against both natural and artificial dangers. The guidelines extended the protection of governmental international organizations (Part B).

"The International Review of Criminal Policy: United Nations Manual on the Prevention and Control of Computer-related Crime" called for further international work and presented a proper statement of the problem. It stated that at the international level, further activities could be undertaken, including harmonizing substantive law, and establishing a jurisdictional base.^{[43](#)}

The Background Paper for the Workshop on Crimes Relating to the Computer Network at the Tenth UN Congress on Prevention of Crime and Treatment of Offenders proposed two levels of definition of cybercrime: In the narrow sense, that is, the strict computer crime, had to refer to "any illegal behaviour directed by means of electronic operations that targets the security of computer systems and the data processed by them." In the broad sense, that is, computer-related crime denoted "any illegal behaviour committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession, offering or distribution information by means of a computer system or network."^{[44](#)}

The UN General Assembly has endorsed several resolutions dealing with its desire to witness progress regarding this issue. According to information provided by [Schjølberg and Hubbard](#) (2005), checking Resolutions 55/63 (2000) and 56/121 (2001) on Combating the Criminal Misuse of Information Technology, the value of the Group of Eight Principles was noted, and states were urged to consider these principles; checking Resolutions 53/70 (1998), 54/79 (1999), 55/28 (2000), 56/19 (2001), 57/53 (2002), 57/239 (2002), 58/32 (2003), and 58/199 (2003), all calling on member states "to promote the multi-lateral consideration of existing and potential threats in the field of information security, as well as possible measures to limit the threats."^{[45](#)} These resolutions have the same motive to improve the cybersecurity

awareness at both the international and the national levels.

In Resolution 55/63, the General Assembly noted the value of the following measures to combat computer misuse:

- a. To ensure the elimination of safe havens for cybercriminals;
- b. To coordinate cooperation in the investigation and prosecution of cybercrime;
- c. To exchange information for fighting cybercrime;
- d. To train and equip law-enforcement personnel to address cybercrime;
- e. To protect the security of data and computer systems from cybercrime;
- f. To permit the preservation of and quick access to electronic data pertaining to particular criminal investigations;
- g. To ensure mutual assistance regimes for the timely investigation of cybercrime and the timely gathering and exchange of evidence;
- h. To remind the general public of the requirement to prevent and combat cybercrime;
- i. To design information technologies to help to prevent and detect cybercrime;
- j. To take into account both the protection of individual freedoms and privacy and the preservation of the capacity of Governments to fight cybercrime.

The General Assembly invited states to consider the measures in their endeavor to fight the criminal misuse of information systems, and decided to maintain the question of the criminal misuse of information technologies on the agenda of its future session.

In Resolution 56/121, the General Assembly invited states to consider the work and achievements of the Commission on Crime Prevention and Criminal Justice and of their international and regional organizations when developing national law, policy and practice to prevent cybercrime.

The resolution emphasized the value of the measures set forth in Resolution 55/63, and again invited states to take them into account in their efforts to combat the criminal misuse of information technologies. However, the General Assembly decided to postpone consideration of this subject, pending work considered in the plan of action against high-technology crime of the Commission on Crime Prevention and Criminal Justice.

It is necessary to mention that, besides the advantages, the disadvantages of the UN's actions are also striking. The UN is a multifunctional international organization, which in some sense has malfunctioned over the years. Focusing on the current topic, it can be said that the consensus on cybercrime in this forum remains a preliminary one. The diversified legal systems of members of this gigantic organization hinder the conclusion of a fruitful agreement.

The focuses of international harmonization

From the above presentation on international actions in anti-cybercrime areas, we can further summarize the major themes of these international organizations. These aspects mainly include the promotion of security awareness at both the international and national levels, the harmonization of legislation, coordination and cooperation in law enforcement, and direct anti-cybercrime actions.

(i) Promotion of security awareness at the international level

The typical actions in this aspect have been taken by the UN. The UN's two Resolutions (55/63 (2000) and 56/121 (2001)) on Combating the Criminal Misuse of Information Technology recalled the importance of the Group of Eight principles, and

urged states to take these principles into account. Some other resolutions also called on member states to promote the multi-lateral consideration of existing and potential threats in the field of information security, as well as promising measures to limit these threats. Other international organizations also made efforts to promote security awareness at the international level. For example, after the 9/11 incidents, the APEC Leaders called for a reinforcing of APEC activities to protect critical infrastructure.

(ii) Promotion of security awareness at the state level

All international organizations have made efforts to promote security awareness at the domestic level. For example, the APEC guided its member states and regions to promote cybersecurity and tackle the threats of cybercrime. The APEC also conducted a project for developed states to support other states in training personnel. The Shanghai Declaration of 2002 supported measures to fight against misuse of information.

(iii) Harmonization of legislation

Legal harmonization has been a major emphasis on the work of various international organizations. Harmonization in Europe started in the 1980s and a recent achievement was the Convention on Cybercrime. Other international organizations have also endeavored to attain legal harmonization. Early in 1981, Interpol surveyed the criminal laws of member states so as to explore defects in the existing legislation, and made efforts to harmonize the laws. Today, Interpol's African Working Party on Information Technology Crime Projects is trying to persuade the African states to sign and ratify the Convention on Cybercrime. APEC also took steps to survey the laws and to encourage economies to enact comprehensive laws consistent with the Convention on Cybercrime and the pertinent UN resolutions. The EU Framework Decision of 2002 specifically granted the member states the responsibility of criminalizing the offences of illegal access to and illegal interference with information systems. The REMJA urged states to criminalize cybercrime and harmonize the member states' laws, and consider the possibility of joining the Convention on Cybercrime. The Commonwealth Model Law on Computer and Computer Related Crime expanded the criminal liability of the Convention on Cybercrime so as to include reckless liability. Through this Model Law, the Commonwealth made efforts to criminalize cybercrime in the member countries. The Group of Eight Paris Conference discussed the public and private interact with the objective of implementing an international penal code for fighting cybercriminality. The Okinawa Charter on Global Information Society further consented to international collaboration and harmonization concerning cybercrime.

(iv) Coordination and cooperation in law enforcement

Interpol's European Working Party on Information Technology Crime compiled the Computer Crime manual to provide technical guidance in law enforcement. The Convention on Cybercrime also covers cooperative mechanisms in law enforcement against cybercrime. The EU discussed about the retention of traffic data in 2001. The Ministers of Justice or Ministers or Attorneys General of the Americas (REMJA)'s Group of Experts on Cybercrime have been devoted to discover cooperation ways in the Inter-American system to combat cybercrime. The Group of Eight reviewed existing cooperation mechanisms and gaps, and made attempt to discover ways to fill these gaps. The Group urged the states to increase criminalization, prosecution, investigation, and international cooperation. The Denver Summit proposed to promote governments' technical as well as legal abilities to act in response to trans-territorial computer crimes. The Birmingham Summit called for agreement on a legal framework

for evidence preservation and protection of privacy, and for agreements on the international sharing of evidence so as to struggle more effectively against a broad scope of crimes, including cybercrime.

(v) Direct anti-cybercrime actions

The direct international anti-cybercrime actions comprise two fundamental aspects: cybercrime prevention and cybercrime investigation. They have been more valuable before international harmonization in legislation could come into being. Different organizations have taken individual measures with specific emphases. For example, Interpol directly cooperated with credit-card companies to fight against payment fraud. The OECD's *Guidelines for Consumer Protection in the Context of Electronic Commerce* 1999 emphasized the protection of consumers in e-commerce as well as that in traditional commerce. Guidelines for the Security of Information Systems and Networks 2002 called on member governments to "establish a heightened priority for security planning and management", and to "promote a culture of security among all participants as a means of protecting information systems and networks".

From conversation to the European Convention

As one of the most outstanding achievements, international actions bred a comparatively effective implementation: the Convention on Cybercrime and its Protocol. The general purpose of the Convention is laid down in the Preamble as to deter crimes against the confidentiality, integrity and availability of information systems and the misuse of such systems. The purpose of the Protocol is to supplement the provisions of the Convention on cybercrime on the criminalization of acts of a racist and xenophobic nature committed through information systems (Protocol, Article 1).

The Convention has been widely accepted as a landmark, providing for both the substantive and procedural legal frameworks, both the domestic and international level of countermeasures, so as to achieve higher effectiveness in fighting against cybercrimes.⁴⁶

Articles 2-12 of the Convention have required nations to criminalize the activities of illegal access to data and computer systems; illegal interception; data and systems interference; misuse of devices that can be used to enact the aforementioned crimes; computer-related forgery and fraud; content-related offences including child pornography; copyright crimes; and attempt, aiding or abetting. Article 13 of the Convention also establishes corporate liability, and sanctions and measures for these offences. Articles 3-7 of the Protocol requires nations to criminalize the activities of disseminating racist and xenophobic information through information systems. Also to be criminalized is racist and xenophobic motivated threat, racist and xenophobic insult, and in respect of genocide or crimes against humanity, denial of their existence, gross criminalistic approval or justification of them, and the behavior of aiding and abetting them.

The Convention provides two constituent elements for cybercrimes. First, the Convention establishes criminal liability on the subjective element of intent. Sometimes, the constitution of certain offences requires elements such as intent to procure "economic benefit" in computer-related fraud provided by Article 8. Second, the Convention establishes criminal liability on the objective element on act "without right" in all offence provisions.⁴⁷ The problems of what is an act committed intentionally, what is an act with right and without right, are all left to national law interpretation.

The Convention allows domestic laws to provide additional constituent elements, and provides the possibility of a reservation.⁴⁸ Apparently, the Convention fully respects the decision-making of member states on the matter of criminal policy. As a result, we have good reason to worry that this diversified implementation will decrease the consensus on the harmfulness of conducts and increase the possible obstacles to international actions. The negative effect of this kind of provision is expected to diminish the effectiveness of prolonged expensive international negotiation for an agreement, although the provision itself is exactly one of the contents negotiated and agreed upon.

The Convention has also been criticized by civil liberties groups concerned that it will undermine individual privacy rights and that it expands too greatly surveillance powers, and is fundamentally unbalanced. As [Taylor](#) (2004) pointed out, the Convention contains comprehensive, far-reaching powers of surveillance, search, and seizure, while lacking a criterion for the protection of privacy and limitation of power.⁴⁹ The basic concerns in the field of human rights are the over-expansion of the states' power of surveillance, and over-criminalization of citizens' behavior. Before information systems have been completely developed, the states would strictly take this borderless system under control; those who use information systems would voluntarily enter the tight legal encirclement. For those who use information systems before these legal instruments, they are to accept externally imposed constraints; while for those who use information systems after these provisions, they are born into an inherent limitation. Both these two groups of users may feel a loss of freedom of information.

Despite the anxiety mentioned above, the Convention has unquestionably had some influence on the worldwide consensus in relation to the predicament of cybercrime. We are capable of seeing that the Convention will become one of the important steps towards a broader international accomplishment.

Firstly, some countries have taken practical measures to ratify the Convention. The total number of ratifications and accessions is 19 countries, including one non-member state of the Council of Europe, the U. S., with 24 countries (including three non-member states of the European Council, Canada, Japan and South Africa) having signed the Convention, not followed by ratifications.⁵⁰ The treaty has entered into force in only a small number of countries, representing a small proportion in terms of land area and population. However, it is still an important step towards a broader consensus: "A little is better than none."

Secondly, besides successful endeavors, countries, including most signatory countries, are still on their way to ratifying the treaty. The Council of Europe Conference on "Cybercrime: a Global Challenge, a Global Response" in 2005 "strongly encourage states to consider the possibility of becoming Parties to this Convention in order to make use of effective and compatible laws and tools to fight cybercrime, at domestic level and on behalf of international co-operation."⁵¹ The treaty has come into force in some of the Nordic countries, including Denmark, Iceland, and Norway, but Finland and Sweden are still seeking ratification though they were both countries of signature on the date opening for signature in 2001.⁵²

However, this process has proved hard without the expected number of countries ratifying in the five-year period after the Convention was open to signature. The pressure against not ratifying the treaty coming from inside the countries seems to be a greater obstacle than the differences over the drafting of the document. A significant obstacle comes from the difference of legislative styles between the

Convention and the individual countries. Many of the valid provisions in current Finnish law do not need revision.⁵³ Whether the original Finnish Penal Code (which includes quite a few revisions concerning offences relating to data processing) is capable of dealing with *all* of the offences provided by the Convention has not been tested in judicial practice. But the Finnish legislature will have to add some new provisions to the Penal Code, if it wants to cope with the Convention. Expressly, provisions concerning the offence of interference with and gross interference with the information processing systems, the offence of possession of instruments for cybercrime (covering the computer viruses), the liability for inchoate cybercrime, and for corporate liability, and so forth must be taken in.⁵⁴

The critical challenge of the Convention on Cybercrime to conventional international legal cooperation lies in the absence of a demand for the double criminality criterion. Since this criterion is in decline, individual countries are far from implementing it in domestic law, either. In accepting the Convention, individual countries will therefore have to revise domestic laws in the relevant area.⁵⁵

Some other countries are seeking to remodel the Convention so as to provide a prohibition on the types of conducts and to create procedural and international mechanisms for serving successful investigations and prosecutions of crimes. The flexibilities of the Convention may have a positive effect in leaving to member states the alternative of using different methods and languages in their domestic law. This may actually lead to a wider application of the Convention so as to cover more and diversified legal systems. While the U.S. has asserted that its own domestic law does not need revision, South Africa has implemented substantial criminal provisions in line with the Convention. Japan is considering filling the gap between its domestic law and the Convention. At least, among the APEC economies, Taiwan, the Philippines, and Hong Kong are considering taking the Convention as the basis on which they will carry out their own legislative amendments.

Some international organizations are propelling cooperation in promoting the member states' access to the Convention. As mentioned above, in the framework of Interpol, the African Working Party on Information Technology Crimes is working to promote domestic legislation and adherence to the Convention. APEC, the EU, and the REMJA V of the OAS have also taken measures to spread the Convention to its member states.

There are also efforts to develop cybercrime legislation beyond the Convention. As mentioned above, the Commonwealth's model law represents a breakthrough in extending criminal liability to the *mens rea* of offences of interfering with data, interfering with computer systems, and illegal devices so as to include reckless liability. Some of the Commonwealth's member states are also on their way towards legislation that will model the Convention and model domestic law.

Finally, in fact, most countries, particularly countries where cybercriminals are usually left at large, have taken no action in spite of the importance of the Convention. These countries have very specific interests in maintaining what may be considered "criminal" in other countries but are "legal" in their own countries, as far as web sites, services, or even sales of goods online are concerned. The potential cybercrime perpetrators, regardless of whichever nationality they belong to, also seek asylum in such countries in order to escape punishment by countries that are seeking to extend their judicial arms to deal with cases committed inside their sovereign territory and committed by their citizens outside their territory.

Although the Convention on Cybercrime has been attracting increasing attention at

both the domestic and international levels, it is necessary to point out that, once the Convention was in documentary form, the enthusiasm and efforts of other international entities towards a higher degree of international harmonization of legislation have been to some extent weakened. This situation reflects neither the purpose, nor the intended side effect of the Convention. However, a ready instrument must have its negative influence on the otherwise unsettled disputes of the problems of cybercrime deterrence. Regrettably, both the advantages and disadvantages of the Convention will bring about a more cautious discussion and a better plan will be discouraged from being implemented. At least, the similar but different schedules for international treaties, in either broader or narrower scope, have seen an interruption with the passing of the Convention. The Convention thus becomes not only a mutual compromise of member states, but also a turning-point in the knowledge and experiences of cybercrime punishment and prevention.

Traditionally, new legal instruments have usually been the subject of academic annotation immediately after its implementation, while the legislature is usually reluctant to change existing legal instruments. These two factors further determine the unfortunate fate of the better and newer proposals, particularly proposals having more or less better elements than the implemented one. In a word, we can say that classics were good, but classics hinder better classics; consensus is good, but consensus always hinders better consensus: and the Convention is good, but it potentially hinders a better convention.

Although the Convention was also appraised by politicians, such as the U. S. President George W. Bush, as "providing for broad international cooperation in the form of extradition and mutual legal assistance", and containing "safeguards that protect civil liberties and other legitimate interests" ([Bush](#), 2003), the effectiveness of the Convention's cooperative framework is subject to reasonable doubt without a majority of countries' access to the agreement ([Goldsmith](#), 2005, p. 4). Authors such as [Archick](#) (2004) have proposed that the Convention's arm would not be long enough to reach the countries that are regarded as a "haven" for cybercriminals: attacks are launched from those countries, but the countries do not join the agreement. Consequently, the countries with law and without law, or being the member and being non-member of the Convention, have to encounter mutual conflicts. The situation confronting international society is obviously still one of the tardiness of the acceptance of existing instruments and the lack of a universal agreement.

The limited progress in the international harmonization

Over the years, the international co-operation on cybercrime "has been very active and comprehensive" ([Pihlajamäki](#), 2004, p. 286). The international level of consensus on criminal law has, however, not been achieved. Previously, the criminalization of war crimes, crime against peace, crimes against humanity, genocide, torture, and other crimes have been the successful examples. The application of pertinent agreements in specific courts has demonstrated that an international forum can acquire certain achievements prior to legislation at the national level. Traditional international criminal law has aimed at harmonizing substantive law and coordinating procedural law on offences that have existed in society since the coming into being of humankind.⁵⁶ Presently, what the countries are eager to realize is an international agreement on offences with a history of only several decades. The anxiety for success, the absence of trial practice, the lack of an accumulation of experience and knowledge, the alienation between the legislature and general public, and the different interests between the various countries, all deliver an international consensus in its lowest form. It is inevitable that during the drafting stage and particularly after the Convention on Cybercrime has been opened for signature, many

commentators have published their evaluation and criticism.⁵⁷ Combined with other progress made in international harmonization, the most important unsolved problem may be the limited participation and the limited consensus.

Firstly, international harmonization has hitherto been primarily the forum of the developed countries. The working mechanism of an effective international treaty is for all of the signatory countries to take effective action and preserve a common theatre of operation. The treaty is not aimed at any third party and thus the third party is not restrained by it. The participating countries of the Convention on Cybercrime are limited, representing only a limited population. Along with the development of the Internet globally, the number of cybercrimes will be correlated with the population base of Internet penetration, and the global population base. Most of the present international harmonization measures have not been incorporating the countries with the largest population. This will make the measures less effective. Considering the characteristics of cybercrime, the "safe haven for criminals" can only be eliminated when almost all the sovereign states have access to one agreement and almost all the online users are subject to the power of law enforcement. Although an international document can be modeled by member states when making domestic laws, the expectations should not be raised too high in respect of a timely update at a similar pace when it comes to international measures.

Secondly, another limitation is that a lower level of consensus has been reached. Unlike traditional offences in international criminal law, which have rarely been penalized in domestic law, cybercrime was initially devised in the legislation at the national level. In many countries, domestic legislation on offences such as genocide, crime against peace and similar types of crime did not happen before the countries were subject to the obligation of international treaties. The situation of cybercrime is that countries that have already enacted laws assisted or forced the countries that have not enacted laws to enter a consensus. As a whole, international cooperation in preventing cybercrime is more sluggish than domestic legislation; its impact on domestic legislation is, nonetheless, undeniable. Domestic laws should be amended according to international instruments so that the measures provided in the international instruments can be effectively carried out. An agreement on a wider scope of issues in cybercrime is also necessary so as to ensure effective law enforcement. However, such an agreement is still lacking. The efforts of various international organizations should be integrated into a more unified action.

Thirdly, there is, strangely, a tendency towards pluralization on the international harmonization. In regulating or deregulating the information community, different interest groups stay at different standpoints. In criminalizing and decriminalizing the online activities, different players hold different opinions. Different organizations propose countermeasures for the benefit of a certain number of their member states. Yet other organizations oppose any kinds of plans for imposing constraints on the free use of information systems. The mechanism is that while one interest group is anxious about the misuse of information systems, another group may concentrate on the side-effect of anti-misuse actions. Various international harmonization measures are full of a trade-off of interests and a contrast of powers. This marathon process of negotiation has inherited the inherent style of international actions.

Fourthly, another tendency is the regularization of international harmonization. The effect of international harmonization is less significant compared with the efforts. The role of the UN as a universal international organization seems limited to arranging an international treaty in this area. If the United Nation's frequent "call" does not motivate member states to legislate on cybercrime, a universal agreement would be a better alternative in promoting consensus. The UN may have the opportunity to

incorporate the consensus reached in other fields into the above-mentioned unified action.

Conclusion

Globalization does not mean globalized welfare at all. Globalized information systems accommodate an increasing number of trans-national offences. The network context of cybercrime makes it one of the most globalized offences of the present and the most modernized threats of the future. We can take actions in two different ways to resolve this problem. One is to divide information systems into segments bordered by state boundaries. The other is to incorporate the legal system into an integrated entity obliterating these state boundaries. Apparently, the first way is unrealistic. Although all ancient empires including Roman, Greece, and Mongolia became historical remnants, and giant empires are not prevalent in current world, the partition of information systems cannot be an imagined practice. Information systems become the unique empire without tangible territory.

Offences occurring in information systems are not likely to receive punishment from this system. Rather, they are punishable by the territory-based states that they cross. It is increasingly stringent and necessary to establish an international cooperation system for punishing cybercrime. Various international organizations have taken actions to resolve the problem in different forums and at different levels.

The Convention on Cybercrime is acknowledged as a landmark in the sphere of the international harmonization of cybercrime law.⁵⁸ However, apart from the fact that it represents a significant step forward, more states will have to sign the Convention and abide by its mandates in order to serve as a deterrent. International harmonization centered on the convention is obviously limited and must necessarily be extended to more participating member states with an even wider scope of issues. The final effect should be achieved only through a universal agreement on combating cybercrime. The UN may have higher potential to implement such universal measures. However, we should not expect an instantaneous reaction from any of the international organizations, because not too much attention and interests of these international organizations are concentrated on the problem of crime or precisely, on cybercrime. While these organizations are devoted to dealing with the more important international affairs, threats against a critical information infrastructure will become more serious, until they are listed at the top of these organizations' schedule. Consequently, the development of an international level of consciousness and an international level call for a national level of consciousness are still the grounds for effective actions. The need is to reassess and renew as necessary the present international legal frameworks, offering a forum for broader international discussion expressing an outlook towards increasing and advancing international law-enforcement cooperation among the national authorities. This development should consider the influences of the novel and emerging issues in respect of international law-enforcement cooperation, with recommendations on capacity-building, which should show an equal concern for the situation in countries at different stages of development so as to avoid a futureless future of information chaos.

Acknowledgements

The author thanks Finnish Cultural Foundation, Jenny and Antti Wihuri Foundation, Turku University Foundation, and Figura-Tuote Oy for financial support for his research, in which the content of this article is included.

References

- APEC (2003). *Conference Report: Cybercrime Legislation and Enforcement Capacity Building Project*, 21-25 July 2003, Bangkok, Thailand.
- Archick, K. (2004). *Cybercrime: The Council of Europe Convention, CRS Report for Congress*. Order Code RS21208, Congress Research Service, 22 July.
- Bourne, R. (2002). *Commonwealth Law Ministers' Meeting: Policy Brief*. London: Commonwealth Policy Studies Unit.
- Bush, G.W. (2003). *Message to the Senate of the United States on the CyberCrime Convention*, Office of the Press Secretary, 17 November.
- Commission of the European Communities (2002). *Proposal for a Council Framework Decision on Attacks against Information System*, COM (2002) 173 final, 2002.
- E-Security Task Group (2003). *E-Security Task Group, Cybercrime Legislation and Enforcement Capacity Building Project*, 21-25 July, Bangkok, Thailand.
- European Union Forum on Cybercrime (EUFC) (2001). *Discussion Paper for Expert's Meeting on Retention of Traffic Data*, Brussels.
- Fooner, M. (1989). *Interpol: Issues in World Crime and International Criminal Justice*. New York and London: Plenum Press.
- Goldsmith, J. (2005). The Internet and the Legitimacy of Remote Cross-Border Searches, *Chicago Public Law and Legal Theory Working Paper*, number 16, The Law School, The University of Chicago.
- Grabosky, P.N. (2004). Global Dimension of Cybercrime, *Global Crime*, 6(1), 146-157.
- Jones, C.W. (2005). Council of Europe Convention on Cybercrime: Themes and Critiques. *Workshop on the International Dimensions of Cyber Security*, hosted by the Georgia Institute of Technology and Carnegie Mellon University, 6-7 April.
- McConnell International (2000). [Cyber Crime . . . and Punishment?](http://www.witsa.org/papers/McConnell-cybercrime.pdf) Archaic Laws Threaten Global Information: Archaic Laws Threaten Global Information. December. Retrieved 18 August 2007, from <http://www.witsa.org/papers/McConnell-cybercrime.pdf>
- Organization for Economic Cooperation and Development (2002). *Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security*.
- Pihlajamäki, Antti (2004). *Tietojenkasittelyrauhan rikosoikeudellinen suoja: datarakoksia koskeva saantely Suomen rikoslaisissa* (The Protection of Data Processing under Criminal Law: Provisions on Data Crimes in the Finnish Criminal Code), Helsinki: Suomalainen lakimiesyhdistys.
- Police Commissioners' Conference Electronic Crime Working Party (2000). *The Virtual Horizon: Meeting the Law Enforcement Challenges: Developing an Australasian Law Enforcement Strategy for Dealing With Electronic Crime*. Scoping Paper, Adelaide: Australasian Centre for Policing Research, Report Series No: 134.1.
- Putnam, T.L., & Elliott, D.D. (2001). Chapter 2- International Responses to Cyber Crime. In: Abraham D. Sofaer, and Seymour E. Goodman, (Eds.), *The Transnational Dimension of Cyber Crime and Terrorism*, Hoover Institution, pp. 35-68.
- Schjølberg, S., & Hubbard, A.M. (2005). Harmonizing National Legal Approaches in Cybercrime, 10 June 2005, *International Telecommunication Union, WSIS Thematic Meeting on Cybersecurity*, Geneva, 28 June-1 July.
- Schjølberg, S., & Tingrett, M. (2004). Computer-Related Offences- A Presentation at the Octopus Interface 2002. *Conference on the Challenge of*

Cybercrime, 15-17 September, Council of Europe, Strasbourg, France. Retrieved 18 August 2007, from <http://cybercrimelaw.net/documents/Strasbourg.pdf>

- Sieber, U. (1996). *Computer Crime and Criminal Information Law - New Trends in the International Risk and Information Society*. Statement for the Hearing on Security in Cyberspace of the United States Senate, Permanent Subcommittee on Investigations, Committee on Governmental Affairs, 16 July.
- Sieber, U. (1998). *Legal Aspects of Computer-Related Crime in information Society, The COMCRIME-Study for the European Commission*, 1 January.
- Sofaer, A.D., et al. (2000). A Proposal for an International Convention on Cyber Crime and Terrorism, Centre for International Security and Cooperation.
- Sofaer, A.D., & Goodman, S.E. (2005). *The Transnational Dimension of Cyber Crime and Terrorism*. Hoover Press.
- United Nations Crime and Justice Information Network (UNCJIN) (1999). International Review of Criminal Policy -United Nations Manual on the Prevention and Control of Computer-Related Crime. *International Review of Criminal Policy*, nos. 43 and 44.
- Wasik, M. (1991). *Crime and the Computer*. Oxford: Clarendon Press.

Endnotes

1. For a general analysis of Interpol as "a world crime-fighting organization that has puzzled three generations of scholars, law-enforcement officers, and legislations," see [Fooner](#) (1989).
2. See [Interpol web site](#) for detailed introduction to the functions and activities of these working parties and the steering committee. Available at <http://www.interpol.net/Public/TechnologyCrime/WorkingParties/Default.asp>
3. Ibid.
4. Ibid.
5. Interpol, Interpol press release, CPN02/00/COMandPR, 5 February 2001.
6. Cybercrime Expert Group, Proposal, Doc No: telwg29/ESTC/12, APEC Telecommunications and Information Working Group, 29th Meeting, 21-26 March 2004, Hong Kong, China.
7. APEC Leaders Statement on Counter-terrorism, APEC Economic Leaders' Meeting, Shanghai, 21 October 2001.
8. APEC, Recommendation by the APEC Telecommunications and Information Working Group (TEL) to APEC Senior Officials (SOM) for an APEC Cybersecurity Strategy, 2002/CSOM/052, Concluding Senior Officials Meeting, Los Cabos, B.C.S., Mexico, 21-22 October, 2002.
9. Ibid.
10. Cybercrime Expert Group, Proposal, Doc no: telwg29/ESTC/12, APEC Telecommunications and Information Working Group, 29th Meeting, Hong Kong, China, 21-26 March 2004.
11. See APEC, Cyber Security Workshop Summary, 2003/SOMIII/ECSG/021, Electronic Commerce Steering Group Meeting Phuket, Thailand 15-16 August 2003.
12. APEC, Conference on the Strengthening International Law-enforcement Cooperation to Prosecute Cyber Criminals, Hackers, and Virus Authors, Media Release, Bangkok, 25 July 2003.
13. Article 26 of Lima declaration, The 6th APEC Ministerial Meeting on the Telecommunications and Information Industry (TELMING, 1-3 June, 2005, Lima, Peru).
14. APEC, 2006 Budget - Operational Account Project: TEL 04/2006 - Judge and Prosecutor Cybercrime Capacity Building Project, 2006/BMC1/012-6, Budget

and Management Committee Meeting I, APEC Secretariat, Singapore, 29-30 March 2006.

15. For example, on 13 September 1989, the Committee of Ministers of the Council of Europe adopted Recommendation R (89) 9 of the Council of Europe on Computer-Related Crime, which contained guidelines for national legislatures.
16. See Council of Europe, Convention on Cybercrime, CETS No.185, status as of 20 March, 2006.
17. Council of Europe, Conference on The Challenge of Cybercrime, 15-17 September 2004, Palais de l'Europe, Strasbourg, France.
18. Council of Europe, Cybercrime: A Global Challenge, A Global Response, Casa de America, Madrid, Spain, 12-13 December 2005, CYB (2005) Conclusions.
19. European Commission, EU Forum on Cybercrime, Plenary session, Brussels, November 27, 2001.
20. Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems, Official Journal L 069, 16/03/2005 P. 0067-0071.
21. Article 1, Joint Action 98/733/JHA of 21 December, 1998 adopted by the Council on the Basis of Article K.3 of the Treaty on European Union, Official Journal L 351, 29 December, 1998.
22. HE 153/2006, Detailed Justifications, 2. Framework Decision and Valid Legislation.
23. Ibid.
24. Meeting of Ministers of Justice or of Ministers or Attorneys General of the Americas (REMJA II), Chapter V.
25. The First Meeting and Second Meeting were held in May and October 1999, separately, the Third Meeting in June 2003, the Fourth Meeting in February 2006, all in Washington D. C. U. S. see [OAS web site](http://www.oas.org/juridico/english/cyber_experts.htm), at http://www.oas.org/juridico/english/cyber_experts.htm
26. Meeting of Ministers of Justice or of Ministers or Attorneys General of the Americas (REMJA III), Chapter IV.
27. Meeting of Ministers of Justice or of Ministers or Attorneys General of the Americas (REMJA V), Appendix I.
28. AG/RES. 2040 (XXXIV-O/04), Adopted at the fourth plenary session of the Organization of American States General Assembly held on 8 June 2004 in Quito, Ecuador.
29. Legal and Constitutional Affairs Division Commonwealth Secretariat, Report on Law and Technology Workshop for the Caribbean, Kingston, Jamaica, 3-7 November, 2003, published in January, 2004.
30. Ibid.
31. Ibid.
32. Ibid.
33. Commonwealth Secretariat, The Harare Scheme on Mutual Assistance in Criminal Matters: Possible Amendments to the Scheme and Discussion of Interception of Communications and Related Matters, Meeting of Commonwealth Law Ministers and Senior Officials, Accra, Ghana, 17-20 October 2005. Annex 1: Summary of recommendations of the Expert Working Group, R4, p. 5.
34. G7, Chairman's Statement, 17 June 1995, Halifax Summit, 15-17 June 1995.
35. P8 Senior Experts Group, 40 recommendations to Combat Trans-national Organised Crime, Paris, 12 April 1996, Reference: 1996CIIa5.
36. G8, Communiqué, Denver, 22 June 1997, Denver Summit of the Eight, 20-22 June 1997.
37. December 1997, the G8 Meeting of Justice and Interior Ministers.
38. Ibid.
39. G8, Okinawa Charter on Global Information Society, Okinawa, 22 July 2000.

40. Ibid.
41. Computer-Related Crime: Analysis of Legal Policy, ICCP Series No. 10, 1986. Cited in UN, Crimes related to Computer Networks: Background Paper for the Workshop on Crimes Related to the Computer Network, Tenth UN Congress on the Prevention of Crime and the Treatment of Offenders, Vienna, 10-17 April 2000, A/CONF. 187/10.
42. See UN General Assembly Resolution A/RES/51/162 (30 January 1997).
43. United Nations Crime and Justice Information Network (1999), Paragraph 295.
44. UN, Crimes Related to Computer Networks: Background Paper for the Workshop on Crimes Related to the Computer Network, Tenth UN Congress on the Prevention of Crime and the Treatment of Offenders, Vienna, 10-17 April 2000, A/CONF. 187/10, p. 5, paragraph 14.
45. See UN web site.
46. Convention on Cybercrime, Preamble, Paragraph 9.
47. Convention on Cybercrime, Articles 2-12.
48. Ibid, Articles 40 and 42.
49. Taylor, G. [The Council of Europe Cybercrime Convention: A Civil Liberties Perspective](#), 23 July 2004. Retrieved 15 March 2007, from http://crime-research.org/library/CoE_Cybercrime.html
50. See Council of Europe, Convention of Cybercrime, CETS No. 185, Chart of Signatures and Ratifications, 19 February 2007.
51. Council of Europe, Conclusions of the Council of Europe Conference on "Cybercrime: a Global Challenge, a Global Response", Madrid, 12-13 December 2005.
52. See, for example, the Governmental Proposal HE 153/2006 of Finland, which aims at bringing the Convention on Cybercrime and the European Union's Framework Decision on Attacks against the Information System into force in Finland and making relevant revision in domestic provisions according to the Convention (HE 153/2006, 3. Objectives and Central Proposals).
53. HE 153/2006, Detailed Justifications.
54. HE 153/2006, General Justifications, 3. Objectives and Central Proposals.
55. Ibid.
56. The origin of human beings has been an unsolved theoretical problem. Genesis theory and evolutionary theory might be the most influential arguments.
57. For an overall evaluation on the Convention on Cybercrime, see [Jones](#) (2005). The Convention was also subject to criticisms from individuals and organizations, such as the American Civil Liberties Union and others.
58. See the Council of Europe Cybercrime Conference, Conclusions, 15-17 September, 2004 High-level Conference on the Challenge of Cybercrime.

Bibliographic information of this paper for citing:

Li, Xingan (2007). "International Actions against Cybercrime: Networking Legal Systems in the Networked Crime Scene." *Webology*, 4(3), Article 45. Available at: <http://www.webology.org/2007/v4n3/a45.html>

Alert us when: [New articles cite this article](#)

Copyright © 2007, Xingan Li.



Toronto Academe Press



9 780973 981308 >